ACSC/DR/007/96-04

CAPSTONE INTERNET POLICY

FOR THE US AIR FORCE

A Research Paper

Presented To

The Directorate of Research

Air Command and Staff College

In Partial Fulfillment of the Graduation Requirements of ACSC

by

Maj Carl D. Baner
Maj James S. Chesnut
Maj Jon N. Link
Maj Ann Marie Matonak
Maj Lani M. Smith

April 1996

01 DECEMBER 1997

POC: AIR WAR COLLEGE.
AIR COMMAND AND STAFF COLLEGE
MAXWELL AFB, AL 36112

Disclaimer

The views expressed in this academic research paper are those of the authors and do not reflect the official policy or position of the US Government or the Department of Defense.

Contents

Illustrations

Page

Tables

Page

Preface

In *War and Antiwar*, the Tofflers describe the knowledge warriors of a third-wave society, stressing that "policies that guide the development and use of information technology in general, and software in particular, are a crucial component of knowledge strategy" (page 169). Even before we were exposed to that concept, we were avid Web "surfers" and believed in the potential of the medium. As it turned out, most of the research conducted for this project was accomplished on-line. There is an immense amount of data on the internet available to anyone who seeks it. In seeking Air Force policy, however, our team developed the impression that all of the current policies, where they existed, were either weak or inadequate for future developments.

We would like to take this opportunity to thank all the people and organizations who spoke with us and were so helpful reviewing our draft ideas for feasibility. In particular, we are grateful for HQ AF/SCXX; the Air Force Internet (AFIN) program management office (Standard Systems Group) at Gunter Air Force Base (AFB), Alabama; Air Intelligence Agency (AIA) at Kelly AFB, Texas who provided the "Intelink CONOPS;" the 42nd Communications Squadron, Captain Montgomery, Commander Coffman, Major Vargas, and Mrs Nancy Kelso at Maxwell AFB, Alabama; and Major McDowell from Air Force Materiel Command (AFMC) at Wright-Patterson AFB, Ohio. We'd also like to thank Lieutenant Colonel Kelso, our Faculty Research Advisor, who had us spend the first four months *surfing* the Web.

Abstract

Air Force use of the internet, especially via the World Wide Web (WWW or Web), has increased dramatically in recent years. However, Air Force policy for use of this technology has not kept pace with developments, resulting in inconsistent or out-of-date publications at the MAJCOM level and a complete lack of policy at the Air Force level.

The combination of literature search, survey, interview, and debate produced several fundamental areas for improvement. This study found that judicious training of the user and network manager could have the most far reaching effect on Air Force internet productivity. By applying commonly understood standards of professionalism and courtesy to issues such as e-mail, the user has already solved many concerns. Off-the-shelf technologies exist to mitigate the hazard posed by security breaches, while user security awareness will have an immediate effect at no expense. Network managers should energetically advocate the Base Network Control Center concept and funding for simplified and higher capacity networks to meet increased demand from software intensive applications. Notably, presentations as simple as a base-level home page require standardization, as they portray an unmistakable image to a world-wide audience.

To address these issues, this project proposed a baseline policy to be incorporated in a future comprehensive Air Force internet policy. Additionally, this project provides a historical background as rationale for the recommended baseline policy.

Chapter 1

Introduction

Imagine mailboxes crammed so full of junk mail that personal letters are deflected to the gutter and swept away. Imagine thousands of otherwise productive workers staring intently, for hours on end, at video screens that they don't fully understand, merely because they've been told it's "highly encouraged." Imagine five-lane side streets packed with rush hour traffic feeding onto a single-lane freeway—the only freeway out of town. "There oughtta be a law!" you say.

The researchers in this study believed that, in fact, there *oughtta* be a "law." Why? Because the preceding scenarios actually require no imagination; in the Air Force internet environment they are real. Unsolicited e-mails fill Air Force "inboxes" daily, exceeding storage capacities, resulting in important e-mails being undelivered. Countless numbers of Air Force personnel are provided every tool required to exploit the information revolution except one—the most important one: useful guidance. Without guidance, critical opportunities to incorporate vast on-line information are lost. With the rush to explore the vistas of the "information superhighway," an outdated Air Force infrastructure leaves many personnel stuck on the on-ramp, as long lines of internet traffic merge into ever-narrowing lanes. These are only a few examples of the awkwardness that

the Air Force is displaying in its effort to exploit what is possibly the most powerful new organizational tool of the century.

Situation

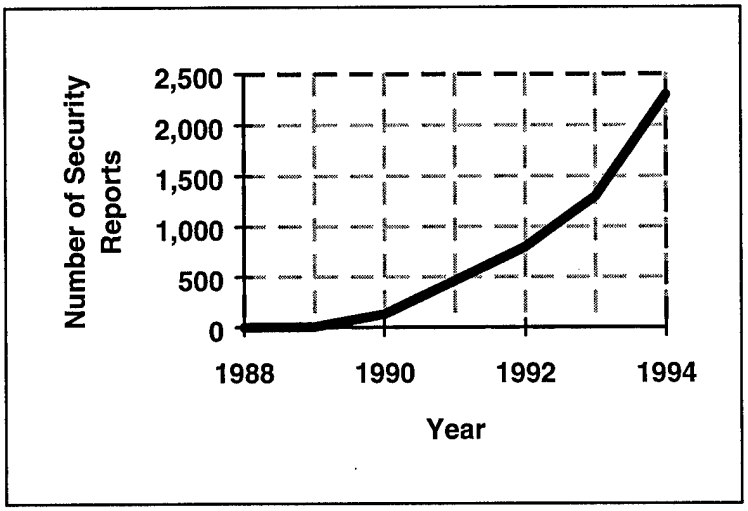
But what is the internet? A definition is appropriate at this point because for many people the internet can mean many different things. For the purposes of this study, the specific protocols supported by the internet are ignored and a more holistic definition is used. *The internet is simply a global connection of networks that are connected to computers, that are "connected" to people.*

From the top down, official guidance for the use of the internet is lacking in substance and centralization. In preparation for this study, a plethora of *more than 30* different official publications were found to relate to the internet and were reviewed. Some policies took a very restrictive slant, effectively denying the user the ability to exploit the technology, while others were merely last year's instruction with a new date. Some policies were published by the top leadership and others by individual units and MAJCOMs. It was obvious that many people had an opinion, but it was also obvious that no one was in charge.

Why is centralized policy so important? Certainly the telephone or the typewriter do not have the requirement for such extensive guidance. The answer is the *potential power* and *rapid growth* of the media of the internet.

The *power* of the internet can leave a person breathless. One minute a person can be typing a letter; the next, checking the weather conditions in Bosnia; and the next, sending e-mail to Headquarters. The potential exists for the user to exploit the media and develop

it into the often sought "force multiplier." It is *possible* with global internet technology for one person to out-perform the work of many. However, with this power comes the potential for abuse. It is easy for personnel to waste time surfing the internet, send unwanted or inappropriate e-mail, or clog a network downloading a large file at the wrong time. Even worse, is the potential for *malicious* intent. Recent surveys, including surveys from the University of Michigan Business School[1] and this study, indicate that *security* is the number one concern of users. This concern is not unfounded. The threat from malicious computer intruders is real; security incidents with respect to the internet are increasing. Figure 1- shows the number of security incidents reported to the Computer Emergency Response Team (CERT) since its inception in 1988.[2]

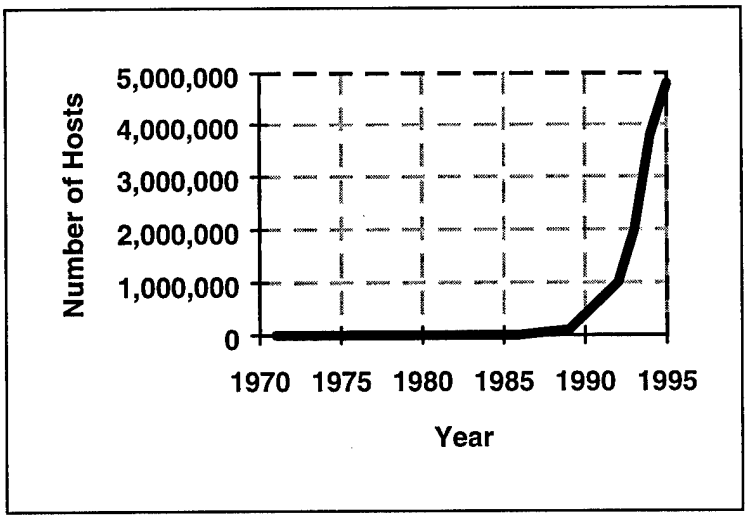


Source: Robert Hobbes Zakon. *Hobbes' Internet Timeline, v2.2*, http://info.isoc.org/guest/zakon/Internet/History/HIT.html. 14 Dec 1995.

Figure 1-1. Number of CERT Security Reports

The incredible *growth* of the internet is also impressive. Although the internet has been around since the 1970s, the relatively recent development of the World Wide Web (WWW, or Web) in 1992 has caused the media to practically explode. The Web has

brought the power of the internet to the common person. Using common "browser" software, a person can click the mouse over a highlighted, or hypertext word, and the hypertext transfer protocol (HTTP) will connect the user to almost anywhere on the globe. Since virtually anyone can use this easy graphical interface with practically any type of computer, the number of people and organizations on-line is growing everyday. One measure of the size of the internet is a count of the number of computer "hosts" or servers on the internet. Figure 1 depicts the explosion of internet use since the Web came on-line.



Source: Kristin Jacobsen, "Time To Put the Internet in Perspective," *C&RL News*, Mar 1995, p144-147.

Figure 1-2. Number of Internet Hosts

Goals

With the above backdrop in mind, this study has two main goals. *First*, new policy will be proposed that is recommended to be the "capstone" of all other internet guidance (see appendix A). The recommendations within this overarching policy will contain specific reference to security and Web issues. The recommended policy is intended to be

inclusive, yet not so restrictive that it does not account for future developments in the technology. *Second*, this study will provide fundamental background and historical information on the internet to support the given recommendations. This study can be read in brief by only reviewing the recommended policies, or can be read in its entirety, where each recommended policy is defended and supported by corresponding analysis and background data. Additionally, internet definitions (see appendix B), internet history, history of security (see appendix C), as well as other issues are provided as general background on the internet.

Framework

This study pursued the goal of a recommended policy by starting with the most important element of the system, the individual user, and proceeding "up" the organization to the network administrator in a manner that eventually percolated an overarching policy at the top. The framework of this paper's progress may be likened to an internet policy "pyramid" (figure 1-3).

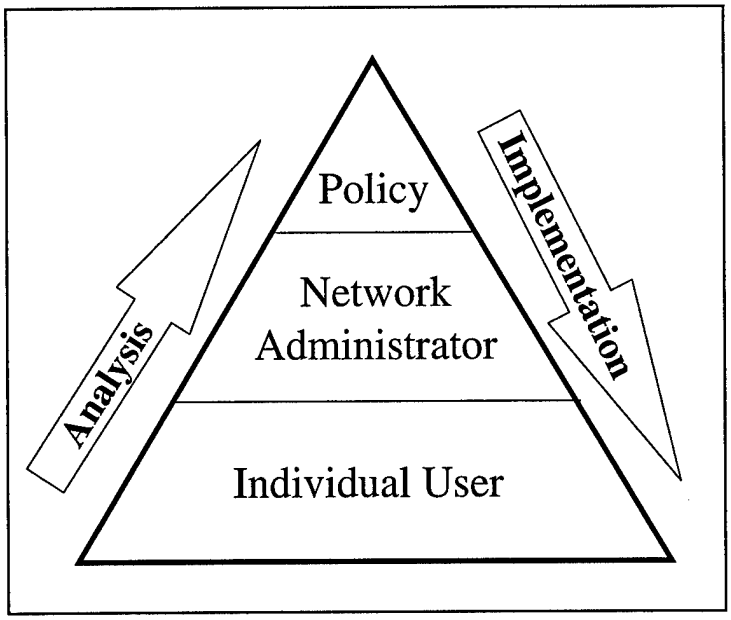


Figure 1-3. Internet Policy Pyramid

Policy affecting the user forms the foundation of the model. Network administrator policy builds on user needs and acts as the intermediary to the global internet. The "capstone" policy, produced from a "bottom-up review" process, is the guidance that fills an apparent vacuum in top-level Air Force policy. It is the thesis of this study that such a policy would have a profound effect on the efficiency and mission effectiveness of the Air Force as it begins to exploit the internet tool.

Chapter 2, "Current Policy Review," initiates the review process by pausing to consider the internet policy "pyramid" as a whole. After noting the conspicuous absence of the crowning capstone, the team saw, from an overall perspective, that the current structure contains widely-spaced and unconnected policies running the depth and breadth of the Air Force. This chapter lists many of these policies, along with several private-sector policies of note. From an inspection of these existing policies, the team developed an appreciation of the current internet environment and the Air Force's part in it.

Chapter 3, "User Policy Analysis," begins the climb up the pyramid model through analysis of the "bedrock" of the internet community: the individual user. In order to formulate a policy that meets the precise needs of the "customer," the team went straight to the source. Surveys of a representative population of Air Force users uncovered a structure made up primarily of individual communications, security concerns, and training issues. All of these elements, and more, were integrated with historical background, real world examples, and case studies producing some insightful results.

Chapter 4, "Administrator Policy Analysis," continues the analysis "ascent" by addressing the middlemen of the internet community: network administration. With the task of providing a bridge between the user and the global internet network, administrators were found to be key to the advocacy of infrastructure concerns. That infrastructure either enhances or stifles the user's exploitation of the internet medium. The study found that the difference was often a fine line.

Chapter 5, "Conclusions," reaches to the top of the pyramid. From a synthesis of all facets of the current Air Force internet policy environment, combined with the survey and research findings of this study, a *capstone* policy emerges and is projected to the notional "Internet Policy" displayed in appendix A. By completing the journey to the top of the Air Force internet policy pyramid, the reader is left with the opportunity to incorporate this study's suggested policy, at Headquarters level, and implement it from the top down.

Scope

A study of any aspect of the internet is a broad undertaking. The internet is a subject that spans the globe. The internet is accessible in nearly every country, and millions of

people, or users, have access to the internet either from work, from home, or from both. Reviewing policy on the internet as a whole is too broad; even analyzing the internet purely from a US or a US government, or even DOD point of view is very broad. This research narrows the focus to aspects of interest to the Air Force community. Even with this narrower focus, the scope is challenging. Originally, this study started as two separate projects: one focusing on Air Force internet security issues and the other on Air Force internet policy issues. It became rapidly evident that these two subjects were related and intertwined. Therefore, the two research groups combined.

The thrust of this project is *not* Information Warfare. Some aspects of this research could be construed as "defensive Information Warfare," because security protection against viruses, hackers and malicious intruders ("crackers") is discussed. Additionally, this research does not address classified computer networks, but rather, the normal unclassified use of the internet by Air Force personnel. Communication of classified information is an important subject, but is outside of the scope of this project.

Research Methods

A goal of this study is to propose a comprehensive, *capstone* Air Force policy concerning use of the internet and all of its sub-capabilities. In order to produce policy that is rational, well-balanced, and durable, several commonly-accepted research methods were used.

To begin the research, a historical examination of related policies and regulations was accomplished. This critical review sought to learn from elements of current internet policies from both private as well as public-sector organizations. The review focused on

the policies of large organizations with concerns similar to the USAF. Existing USAF and DOD publications were also reviewed to determine applicability to an internet policy document. The findings of this review are highlighted in chapter 2. This collection of historical data served as a point of departure for the next research method employed: the descriptive survey (for the remainder of the study, this survey will be referred to as the Research Survey).

To glean the most up-to-the-minute internet issues and to balance the policy with respect to the ultimate "customer," the Research Survey was published and distributed to a representative population of Air Force personnel. The two-page survey asked respondents to describe their views on several internet issues, to include privacy, security, decency, and mission enhancement. The Research Survey also asked for certain demographic and statistical information on frequency of use, services employed, and home use. Within the constraints of time and budget, proctors surveyed a representative cross-section of Air Force personnel that would be most affected by a comprehensive policy. The Research Survey and its results are in appendix D, while knowledge gained from the Research Survey is incorporated throughout this paper. With historical and current data in hand, the next research step explored future considerations through the vision of organic internet "experts."

The "expert" survey method was employed to add technical depth to the study and to explore future trends that could be anticipated in a durable policy. The expert survey was performed by personally interviewing Air Force personnel in key positions applicable to the internet. The interviews were loosely structured and centered on the free flow of

ideas from the interviewee. Interview notes and raw survey data are archived and available from ACSC/DR.

To determine the *specific subjects* for this research, two main sources were used: the review of published guidelines and the Research Survey. A "User Policy Issues Matrix" (see appendix E) was built by summarizing selected guidelines to determine the most common and important issues relevant to USAF personnel. Additionally, the results from the Research Survey (see appendix D) uncovered other issues such as network capacity or bandwidth, standardization, and accessiblity. All of these issues were further broken into two main categories; issues primarily the responsibility of the *user,* and issues primarily the responsibility of the computer *network administrator.* Two subjects that were common between the user and the administrator sides were security issues and the need for training.

All of the above information was then synthesized into the body of research in chapters 3 and 4 through a "problem-solution-recommendation" approach that linked the current situation with corresponding analysis for each discrete element of the overall policy environment. The "solutions" posited in the body are summarized in the "Conclusion" (see chapter 5) and become the entering arguments of the proposed "Internet Policy" (see appendix A).

Notes

[1]"Consumer Survey of WWW Users, Preliminary Results from 4th Survey" (12 December 1995). University of Michigan Business School. [On-line]. Available HTTP: http://www.www.cc.gatech.edu/gvu/user_surveys/survey-04-1995 [1995, December 20].

[2]Richard D. Pethia, Kenneth R. van Wyk, *Computer Emergency Response - An International Problem,* Pittsburg, PA: Computer Emergency Response Team/Coordination Center, Software Engineering Institute Carnegie Mellon University,

Notes

Pittsburgh, PA, (14 November 1990). [On-line]. Available HTTP http://www.riken.jo.jp/archives/security/cert/info/security.response.cert.txt [1996, February 28].

Chapter 2

Current Policy Review

The internet originated as a network of computers designed to facilitate the distribution of research information around the United States. Over the years, that free flow of information fostered a feeling of anarchy. To counter this feeling, organizations that have come to depend on the internet, such as the DOD and the Air Force in particular, have written publications and guidance to help the user and the system administrator. Other organizations, such as private companies, Internet Service Providers (ISP), and universities, have also written guidance to give new users direction and provide knowledgeable users a "box" of allowable behavior to work within. In this chapter, the study steps back from the pyramid model (figure 1-3) and begins the analysis process by reviewing the current collection of internet guidelines and policies.

This chapter is the literature review. Policies and guidance from DOD and Air Force sources, as well as guidance from private sources, are examined. Although a publication is listed, it may not necessarily be cited within the research paper. In this case, the publication was reviewed and did not contribute materially to the topics that are addressed within the paper but was useful as background information. As an interesting note, most of the publications listed within this chapter can be obtained electronically.

Many of the USAF publications can be found on-line or on CD-ROM, and most of the private organization publications can be found on-line.

DOD and USAF Publications

Many existing DOD and USAF publications, guidelines, and policies were reviewed. These Air Force Instructions (AFI), Air Force Policy Directives (AFPD), and guidance letters and publications are listed below in table 2-1. Although all of these publications were reviewed and would seem to have pertinent information in them, it was found that very few actually contributed to the understanding of existing official internet policy. The internet is growing and evolving so rapidly that most existing policies have not kept up. An example of this rapid evolution is the leading edge publication: Air Force Materiel Command (AFMC) Instruction 37-102, *Transmission of Information via the Internet*.[1] When this research project was initiated in November 1995, this instruction did not exist. It was published in March 1996 and not only filled a vacuum within AFMC, but at least three other Air Force agencies liked the draft so well they decided to implement the instruction word for word in their own organizations.[2] Incidentally, this instruction, although available in paper form, was originally released via a Web home page.

Even though many of the publications reviewed did not contribute to the understanding of internet policy, it is obvious that consideration of this problem is a serious matter. Several of the guidelines reviewed were signed by the Deputy Secretary of Defense and the Secretary of the Air Force. Also, it is obvious, just by reviewing the list of publications, that there is no single DOD or Air Force agency publishing

centralized policy on the internet. Instead, there are many directives, publications, and guidelines written by many different organizations.

Table 2-1. Pertinent DOD and Air Force Policies

Document	Brief Description
SecDef Memo, *Clearance Procedures for Making Electronic Information Available to the Public*	17 February 1995. From the Office of the Deputy Secretary of Defense (Mr John M. Deutch).
SecDef Memo, *Open Computing Architectures*	5 May 1995. From the Office of Deputy Secretary of Defense. Maintaining a balance between providing accessibility and secure computer operations.
DOD 5200.1, *Information Security Program*	7 June 1982. Broad guidance on information security.
DOD 5200.21, *Dissemination of DOD Technical Information*	27 June 1982. Broad guidelines for disseminating DOD technical information to avoid duplication of effort and for the benefit of US companies and institutions.
DOD 5230.9, *Clearance of DOD Information for Public Release*	2 April 1982. Provides guidelines and restrictions on DOD information for public release.
DOD 5500.7-R, *Joint Ethics Regulation*	August 1993. Use of Federal Government Telephone systems (paragraph 2-301).
DOD 5500.28, *Security Requirements for Automated Information Systems (AIS)*	21 March 1988. Provides broad general guidance for administration of computer security requirements.
DOD 5500.28-STD, *Department of Defense Trusted Computer Security Evaluation Criteria*	26 December 1985. Often referred to as the "Orange Book." Defines requirements for Air Force computers connected to the internet.
SAF Memo, *Clearance Procedures for Making Electronic Information Available to the Public*	25 May 1995. Memorandum for ALMAJCOM-FOA/CC, from the Office of the Secretary of the Air Force (Ms Sheila E. Widnall).

Table 2-1.—continued

Document	Brief Description
SAF/AQT Memo, *Use of Internet for Transmitting or Providing Access to Unclassified, Limited Distribution Information*	12 December 1994. Unclassified limited distribution information must be encrypted if it is accessible on the internet.
AF Policy Directive (AFPD) 31-4, *Information Security*	1 November 1995. Guidance for protecting sensitive USAF information.
AFPD 33-2, *Command, Control, Communications, and Computer (C4) Systems Security*	13 August 1993. C4 systems security requirements and responsibilities.
AFPD 33-1, *Command, Control, Communications, and Computer (C4) Systems*	17 September 1993. Overall guidance for Air Force C4 systems.
AF Instruction (AFI) 33-114, *Software Management*	30 June 1994. Identifies responsibilities for managing, developing, maintaining, and implementing Air Force software.
AFI 33-115, *Network Management*	24 June 1994. General guidance on the relationships and responsibilities of LAN. Defines the role of the Base Network Control Center (BNCC) and other system administrators.
AFI 33-219, *Telecommunications Monitoring and Assessment Program (TMAP)*	12 June 1995. Includes computer system security warning banner information.
AFI 35-205, *Air Force Security and Policy Review Program*	25 February 1994. Provides for expert review of information proposed for public release to ensure it does not contain classified material or conflict with established DOD or national policy.
AFI 37-131, *Air Force Freedom of Information Act Program*	16 February 1995. Provides guidance for making records public and for the USAF FOIA program.
AFI 37-132, *Air Force Privacy Act Program*	11 March 1994. Sets guidelines for collecting, safeguarding, maintaining, using, assessing, amending, and disseminating personal data kept in systems of records.

Table 2-1.—continued

Document	Brief Description
AFI 37-162, *Managing the Process of Printing, Duplicating, and Copying*	1 December 1994. Covers copier machines and local printing.
AFI 51-303, *Intellectual Property—Patents, Trademarks, and Copyrights*	25 July 1994. How to protect government interests, and procedures when the government wants to use copyright material.
AFI 61-201, *The Local Scientific and Technical Information Process*	16 June 1995. Establishes procedures for local scientific and technical information (STINFO) officers to disseminate information.
AFI 61-204, *Disseminating Scientific and Technical Information*	27 July 1994. General distribution and control requirements for unclassified technical information.
AF Manual (AFMAN) 37-126, *Preparing Official Communications*	10 February 1995. Contains the procedures for preparing communications in the manual and automated environments.
AFMAN 37-126/AFMC Supplement 1	20 July 1995. Includes AFMC e-mail policy.
AF System Security Instruction (AFSSI) 5013, *Password Management*	15 March 1993. Information on password construction: minimum of six random alpha-numeric characters, changed every six months.
AFSSI 5021, *Computer Security Reporting Programs Procedures and Formats*	10 February 1993. Reporting requirements for security incidents and system accreditation.
AFSSI 5100, *The Air Force Computer Security (COMPUSEC) Program*	2 June 1992. Defines roles and responsibilities of C4 systems security at MAJCOM, base, and organization levels.
AF System Security Manual (AFSSM) 5012, *System Vulnerabilities and Penetration Methods*	1 October 1991. Explanation of attacker methods from user, system administrators, maintenance personnel, and hackers.

Table 2-1.—continued

Document	Brief Description
AFSSM 5019, *Computer Security User's Guide*	1 April 1991. Overview of computer security requirements.
AFSSM 5020, *Remanence Security*	15 April 1991. Procedures for clearing and purging data from computer system memories and storage media.
AFMC PD 37-1 *Internet Policy*	19 February 1996. General internet policy guidelines for AFMC.
HQ AFMC OI 37-1, *Information Sharing Through the World-wide Web*	15 March 1996. Operating instructions for HQ AFMC. Provides internet background, threats, and responsibilities.
AF Handbook (AFH) 37-137, *Tongue and Quill* (Draft Inputs)	Use of the internet and e-mail: writing e-mails, internet courtesy, and basic do's and don'ts.
Intelink Concept of Operations for AF-wide Implementation (draft)	25 July 1995. An adaptation of the internet concept, operating in a secure environment, using Web technology. OPR: AIA/SCXP
AF Pamphlet (AFPAM) 36-2705, *Discrimination and Sexual Harassment*	28 February 1995. The Air Force cannot tolerate racial tensions or sexual harassment. Provides insight and guidance for a healthy and productive work environment for all members of the Air Force.

Other Private Agencies

Just as the DOD and the Air Force have policies on internet usage—albeit out-dated, not centralized, and inadequate—other organizations have documented their own "rules of engagement." Self-contained domains such as America Online, CompuServe, or Prodigy are the most restrictive: their guidelines are meant to promote a feeling of community and make the services more family-friendly. Other ISPs, in keeping with the free-wheeling history of the internet, sometimes resist setting down *detailed* acceptable behavior guidelines. Their reluctance does not necessary reflect a belief that guidelines would not be useful. Rather, it seems that they are mindful of possible liability charges.

Nevertheless, there are generic and specific network guidelines available for review. Two products by Ms Arlene Rinaldi are often used in organizational network policies. Rinaldi, an academician at Florida Atlantic University, was one of the first researchers to codify internet "rules of the road" and display them through a highly visible medium on her own Web home page. Her page quickly became one of Point Communication's vaunted "Top 5% Web Sites"[3] and has become the seminal starting point for internet policymakers. The remaining four documents are examples of organizational policies with origins in Rinaldi's *Netiquette*.

Table 2-2. Pertinent Non-DOD Guidance

Document	Brief Description
Rinaldi's *Netiquette*	A general listing of suggested behaviors and network usage rules.
Rinaldi's *Network Computer Policy*	A "contract" between organizational network and user.
America Online, *Rules of the Road* and *Forum Guidelines*	6 December 1995. A detailed list of unacceptable behaviors which can result in censure from the on-line service.
CompuServe Information Service, *Operating Rules*	To help make on-line information usage and communications a positive and secure experience for members.
National Science Foundation Network (NSFNET), *Backbone Network Service Acceptable Use Policy*	17 January 1995. NSFNET Backbone services are provided to support open research and education in and among US research and instructional institutions, plus research arms of for-profit firms when engaged in open scholarly communication and research. Use for other purposes is not acceptable.
Invitrogen, *Electronic Mail Etiquette*	A very general set of rules for polite and acceptable on-line behavior. Also includes a set of mini-"net-ethiquette" case studies.

Notes

[1]AFMCI 37-102, *Transmission of Information via the Internet.* [On-line]. Available HTTP: http://www.afmc.wpafb.mil:12000/publications/AFMC_Instructions/37-102.doc [1996, February 21].

[2]Maj Phil McDowell (mcdowep@WPGATE1.wpafb.af.mil). (1996, February 21). re: Policy and Security Issues. E-mail to Maj Jon Link (jlink@MAX1.au.af.mil).

[3]"Top 5% of the Web." (1996). Lycos Inc. [On-line]. Available HTTP: http://www.pointcom.com/ [1996, March 26].

Chapter 3

User Policy Analysis

"User Policy Analysis" addresses the foundation of the "Internet Policy Pyramid" (figure 1-3): the individual user. As mentioned previously in "Research Methods," the specific subjects that this project addresses were determined after analyzing the internet "User Policy Issues Matrix" (see appendix E) and the results of the Research Survey (see appendix D). This matrix and the Research Survey results highlighted several issues that were common in the selected guidelines and are relevant to Air Force personnel. This list of issues was broken into two broad categories, those issues that are the primary responsibility of the individual user and those that are the primary responsibility of the network administrator. This chapter discusses, analyzes, and provides recommendations for the "user issues." The subsequent chapter similarly addresses the "administrator issues."

Individual Communications

Currently, individual communications via the internet are either text, audio, or video based. In each case the communication is either synchronous or asynchronous. Text and audio are commonly asynchronous, in that the message is a packaged unit sent and received at a later time much like postal mail. The video medium is commonly

synchronous, meaning that the individuals involved converse interactively, or in "real time." There are examples, however, of uncommon use in each media.

Of the more uncommon communications techniques, text based messages may be exchanged via "chat," a synchronous medium where both messages appear on screen as they are being typed. Audio messages may be exchanged via internet "phone" connections where the individuals talk back and forth much as on a telephone connection. Video messages may be sent asynchronously as a pre-recorded video clip. Whereas these applications may be currently characterized as "uncommon" (due mostly to hardware and software limitations), as internet capabilities increase, convergence of audio and video technologies to the internet may obviate current messaging, such as text e-mail, and produce new challenges.

Current Situation

By far the most popular current use of the internet among Air Force personnel is the transmission of text e-mail. Most users were introduced to the internet through mandatory use of e-mail in their offices and remain most comfortable with this medium. According to the Research Survey, e-mail at work was one of the top two internet issues on the minds of respondents, second only to security concerns (see appendix D).

As with any popular communications media, certain standards of conduct have emerged that are commonly accepted amongst the user society. This internet etiquette, referred to as "netiquette" has been codified by several organizations and utilized as policy in some cases. One of the most well known netiquette documents is Arlene H. Rinaldi's *The Net: User Guidelines and Netiquette.*[1]

Rinaldi's policy addresses File Transfer Protocol (FTP) and telnet issues along with e-mail, but spends most of its time on electronic text issues. She concludes with "Ten Commandments for Computer Ethics," hearkening to Asimov's "Three Laws of Robotics."[2] Rinaldi's guidelines synthesize common sense and traditional ethics with the technical realities of the internet medium.

Proposed Policy

From the previous description of Rinaldi's guidelines comes one of the key findings of this study: the conclusion that a truly *durable* internet policy should be evolutionary rather than revolutionary. In other words, much of the best advice on the use of the internet may be based on the wealth of experience that the Air Force, as an evolved technical organization, already has with other media such as telephone, written, or last generation "messaging."

An analysis of several current internet policies from various sources gleaned ever deepening support for the thesis that the common sense approach of Rinaldi's guidelines may be the genetic center of the current internet communications policy universe. The analysis surveyed six internet policy documents (see appendix E). In addition to Rinaldi's, four of the policies were from Air Force sources and one was from a civilian corporation. Of the policies surveyed, the three most popular issues and seven of the eight "second place" issues were common with Rinaldi's guidelines.

The above analysis led this study to the initial conclusion that Rinaldi's guidelines *and approach* should be the basis for the formulation of a Headquarters-level policy that includes individual internet communications. With that in mind, the team then rank-ordered the most popular issues found across the assembled policies and (most

importantly) evaluated those issues against the results of the Research Survey. The final step of filtering through the Research Survey was designed to ensure a policy that was most responsive to the *user*.

Recommendation

The previously described process of comparison and filtering resulted in the final policy recommendation on individual communications that is incorporated in appendix A. The corresponding section of the capstone "Internet Policy" (see appendix A) suggests 14 sound techniques for Air Force e-mail use.

Privacy

One of several internet demons that frighten potential users is the issue of privacy. Privacy and security are very similar issues. For the purposes of this study, *privacy* will be used to define appropriate conduct of the established network on the user. *Security*, on the other hand, will describe measures to foil unauthorized intrusion on network traffic by "outside" elements. As an example, unsolicited e-mails may invade the privacy of a user, while the unauthorized interception of an e-mail by a hostile third party would be a breach of security. This is admittedly a fine line, but more importantly the line must be drawn to determine the appropriate vehicle of policy. Privacy issues may be resolved through local operating restrictions, whereas security issues also rely on physical measures such as firewalls and encryption devices (see "User Security," page 47 and "Administrator Security," page 82).

Current Situation

Like many of the issues affecting the internet, privacy is not unique to the electronic medium. Traditional standards, such as the *Privacy Act of 1974*,[3] apply equally as well to the internet, but are more difficult to observe and enforce. For the purposes of this study, privacy will include the areas of confidentiality, solicitation, and individual precaution.

Confidentiality is a familiar concept in professional circles. For the most part it is a common sense standard that asserts the reliance on another's discretion, most commonly in personal communications. The relative ease with which a confidential internet communication may be copied or redistributed makes this issue particularly problematic.

An example breach of confidentiality might be an e-mail sent to a supervisor involving a question on local leave to resolve domestic problems. The temptation might be for the supervisor to merely "forward" the e-mail to the remaining workers in a section in order to deconflict duty coverage prior to approving the request. But, did the author of the original message intend to broadcast his or her domestic situation to his or her co-workers? And what of the particularly gossipy co-worker who, in turn, re-forwards the sensitive information to several friends? The eventual result of this scenario might be tantamount to announcing an individual's family problems at a commander's call. In the survey of Air Force officers, 10 percent said that they, in fact, had been the victim of embarrassment through the unapproved forwarding of a "personal" e-mail (see appendix D).

While the issue of confidentiality may seem relatively harmless to some, it has a potential impact on both the interpersonal and legal climate of an organization. Internet analyst, Deborah Sawyer summarizes the problem by emphasizing:

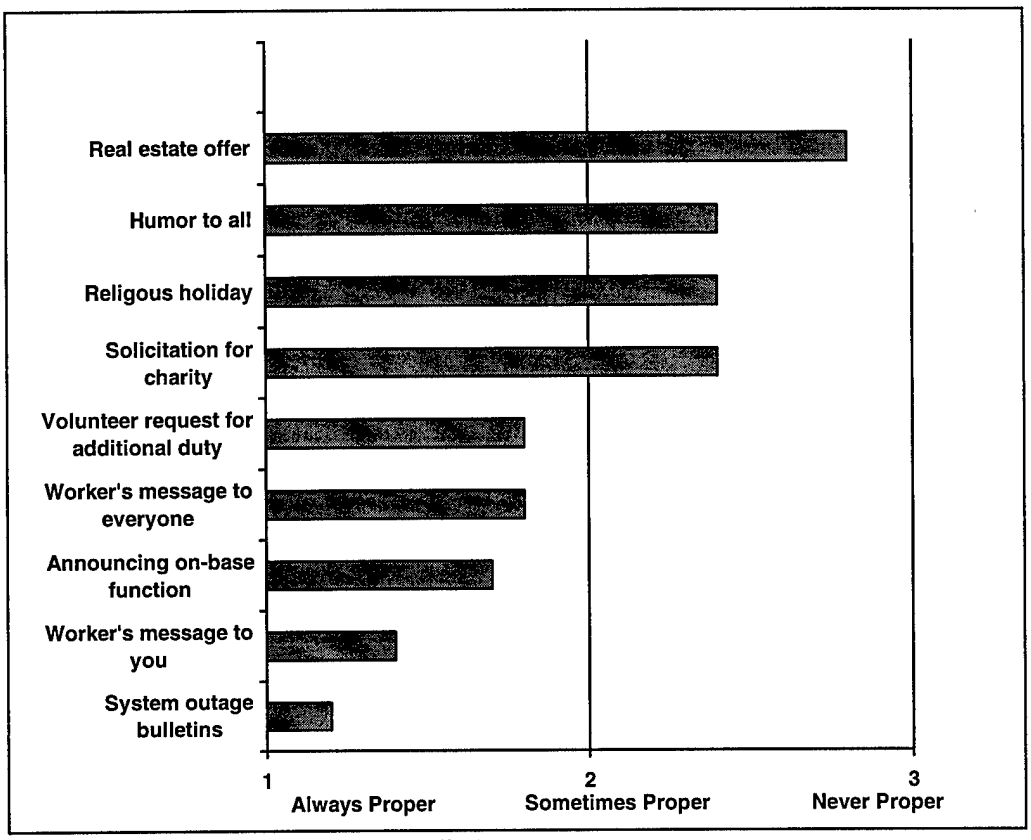
> Confidentiality is the hallmark of professionalism. It is imperative that we protect all confidences that result from professional interactions. Communicating such information on a network (even inadvertently) is much worse than individual or local breaches; the potential harm is greater because the information is broadcast so much more widely. In addition to resulting in ethical culpability, transgressions of this nature are actionable. Liability and malpractice suits are distinct possibilities in this context.[4]

Solicitation refers to the use of digital communications to gain an individual's monetary or non-monetary commitment to the sender's product, task, or cause. Simply stated, someone wants you to do something for them, and in cyberspace they can reach out and tap you on the shoulder like never before. In the past, solicitors were required to "pound the pavement," "put the foot in the door," and *ask* to deliver their "pitch." No more. With electronic mail and similar digital media, the pavement becomes a mailing list. The foot in the door is automatic, and the message is delivered whether you like it or not, complete with automatic "return receipt" to inform the sender of *exactly when* you read it. The implication of this phenomena is sobering. As many Air Force members have already experienced, the concept of "junk mail" has found its way to cyberspace. A typical electronic mailbox may fill to capacity in only a few days, while the receiver vainly attempts to delete incoming letters as fast as they arrive. As with a postal mailbox, the user finds that the vast majority of inbound mail is solicitous in nature and mostly undesired. The Research Survey found that respondents were consistently annoyed by the constant flow of unsolicited e-mails. Unlike the postal analogy, though, on-base e-mail is not, at present, composed of commercial solicitation. What then is clogging up the " mail boxes"?

The Research Survey found that even without commercial solicitation present, solicitation in other forms is rampant *within* the base local network. Examples could

include fund drives, such as the Air Force Assistance Fund (AFAF); additional duty solicitation, such as escort officer duty; cultural heritage activities, and church breakfasts. The question is not whether any one of these activities is legitimate in itself, but whether each and every address should be exposed to each and every solicitation. Where do you draw the line? The Research Survey addressed that question with some interesting results.

The Research Survey asked respondents to judge the "appropriateness" of several categories of e-mails. Of the nine categories surveyed, four could be considered as "solicitations" of varying degrees. Figure 3-1 shows the results by category. The results suggest that the majority of our respondents are indeed sensitive to the *type* of e-mail that clutters their box, and at the least, feel that some categories are simply inappropriate for transmission to the base community.



Source: Research Survey, appendix D.

Figure 3-1. Relative Inappropriateness of E-mail Types

Individual precaution in any type of communication may seem obvious, but like several other issues, the newness of the internet environment has caught many off-guard. It is perhaps ironic, that of all the subjects surveyed in current internet policies, *precaution* is given little time. Indeed, most anecdotal studies, such as the University of Southern Queensland mini-cases referenced in the Invitrogen policy,[5] focus on the "pound of cure" rather than the "ounce of prevention." This focus, however, is awfully risky given the ever increasing on-line population and commensurate potential for personal and organizational harm. In most cases, simple awareness of the potential for "forwarded" e-mails, solicitous tone, and the like will go far in reducing the occurrence of

privacy-robbing events. This awareness requires user training (see also "User Training," page 51) and a brief mention in policy.

Recommendation

Due to the critical importance of confidentiality in the workplace, Air Force policy should restrict the forwarding of electronic messages without the consent of the original author. Concerning solicitation, the capstone policy should forbid commercial (for profit) e-mails under any circumstances, and limit "charitable" (non-profit) e-mails to a discrete audience, such as a squadron. Further, all remaining non-work-related e-mails should be expressly discouraged from wide dissemination. Finally, on the issue of individual precaution, the capstone policy should include a section that emphasizes "safe computing": healthy on-line habits that may preclude the majority of pitfalls that currently exist. Specifically, all personnel should be made aware of the potential for message forwarding, in order to take steps to guard against unwanted exposure.

Cultural Issues

Like privacy, cultural issues are not specific to the internet. Their effect is merely magnified by the ability for workers to more easily transmit or solicit information involving offensive materials. The danger to the organization is two-fold. From within, employees have a semi-anonymous vehicle to vent harassment or hatefulness at light speed. From without, the organizational image is subject to scrutiny each time an employee accesses offensive or controversial material on company time.

Current Situation

> One of the first companies to draft an Internet code of conduct was Wisconsin-based Johnson Controls. The policy forbids Johnson employees from making harassing or offensive on-line statements, including any debasement of race, sex, national origin, sexuality, age, disability and religious or political beliefs. It also prohibited staff from conducting personal business, seeking jobs outside the company, soliciting sex, ... posting sexually oriented messages, ... or raising funds for religious or political causes via company access to the Net.[6]

The effect of a policy such as Johnson's is to bring the employee back to the basic reality that, first, well-established policies prohibiting harassment of any form apply equally to the medium of cyberspace, and second, the employee must be especially vigilant of his or her on-line behavior while representing the company due to the unique dangers involved.

On the first point, it is perhaps somewhat strange that with the advent of a new age in communications technology, academics and the public alike are questioning the form of a new "cyber-morality." Authors Hauptman and Motin rebuke this line of thought by noting that while terms such as "cyberspace" and "virtual reality" may be useful metaphors, the extension of those constructs to create concepts such as "cyberethics" and "virtual morality" are invalid.

> [The terms] Cyberethics and virtual morality are nonsense. They are particularly harmful if they allow us to confuse reality with a nonexistent universe where unethical actions are [presumed to be] permitted. The ethics of human interaction remain constant.[7]

On the second point, internet observers have found that e-mail, for some reason, tends to bring out the more uninhibited side of the sender. Ted Julian, an analyst at International Data Corp. in Massachusetts, says:

> It's a new technology, and it has its own cultural differences that employees should be made aware of. E-mail has a tendency to be less

> diplomatic and more heated, and if what you want to achieve is good relations through the use of the Internet, your employees should be reminded of this.[8]

Proposed Policy

The irony is that inappropriate paper messages within an organization are less easily reproduced and more subject to editorial scrutiny. Conversely then, it is the combination of the ease of reproduction and lack of filtering that makes e-mail messages so potentially dangerous in an organizational society.

Most Air Force employees are well aware of organizational policy on cultural sensitivity. Air Force Pamphlet (AFPAM) 36-2705, *Discrimination and Sexual Harassment* details techniques for recognizing and solving discriminatory problems, to include techniques of effective communication.[9]

Recommendation

AFPAM 36-2705 and related Air Force policies should be referenced in the capstone internet policy with a brief "warning" statement concerning the increased danger of inadvertent discrimination or harassment in the cyber-medium.

Copyrights and Releasability

Not long ago, information was only available in printed form. In those days, the written word was only considered copyright-protected if that right had been claimed and properly registered. This is no longer true.[10]

With the inception of the internet, protection of intellectual property became much more complicated because digital information on the Web is so easily downloaded, modified and re-distributed without degradation. The issue is not limited to words and

ideas. Music and pictures are also available and vulnerable. Hypertext (a highlighted word found on Web pages that links with another Web location) makes it possible for a single site, containing the original upload of a creation, to be queried thousands of times a day, resulting in potential world-wide distribution. The application of copyright law onto electronic media is still hotly argued and of vital interest to creators and "content" providers.

Current Situation

Already, there have been several incidents of intellectual property being distributed or co-opted contrary to its creator's wishes. The following examples demonstrate the wide-spread nature of this "problem."

In 1994, a copy of the script for the feature film *Star Trek: Generations* was uploaded to an internet newsgroup long before production was finished. That action was completely unauthorized by Paramount Pictures, the owners of the script, and kicked off a furious discussion.[11] Some insisted that nothing wrong had been done. A few accepted that the person who uploaded the script acted illegally but then asserted that subsequent downloading of the script was allowable, and still others proclaimed that the original upload was wrong and all the downloads were also improper. Though copyright law for electronic media has not been completely codified, there are several repositories of copyright "frequently asked questions." For example the Air University home page[12] includes a link to the Templeton essay entitled "10 Big Myths About Copyright Explained."[13] Brad Templeton is the Chief Executive Officer of ClariNet, an electronic publishing company, and this essay has been widely distributed around the internet.

More recently, the Church of Scientology used alleged copyright violations as the reason for a lawsuit against a person who had placed scientology information on the internet.[14] And in another instance, the estate of Elvis Presley took action against a fan's unofficial home page containing a "cyber-tour" of Graceland.[15] The results of these lawsuits may clarify the legal rules, but for the time being, the world of copyright rules on the internet is a "zoo," and in some situations it more closely resembles a "jungle."

Copyright laws are not just a US concern. With the eventual development of a global information infrastructure, these rules would have international aspects and implications as well.[16] In March 1996, a book banned in France appeared, in violation of copyright law, on various Web sites. Since the book is banned, French government officials do not seem enthusiastic about aggressively enforcing copyright protection for it.[17] The World Intellectual Property Organization (a Geneva-based group) has scheduled a conference for December 1996 to discuss extending Berne Convention copyright protection to electronically-distributed materials.[18]

Much of this incorporation is already occurring in the United States. In 1988, Congress incorporated elements of the Berne Convention into law so that all *created* works automatically are copyrighted and protected.[19] Then in 1995, recognizing the re-distribution potential of the internet, the White House released a report on "Intellectual Property and the National Information Infrastructure (NII)."[20] One of NII's purpose is to facilitate the establishment of clear rules for intellectual property protection and the creation of technological safeguards. An interagency working group, in association with the US Patents and Trademarks Office, made several Copyright Act modification recommendations to clarify distribution rules.[21]

Those recommendations concern many higher education associations, whose representatives have testified before a House subcommittee, urging the lawmakers to delay passing new electronic copyright rules before the impact of those rules on colleges and universities is assessed. Specifically, schools are concerned about the proposed revised definition of "fair use" of copyrighted digital materials, concerned that it will eliminate or severely restrict on-line interlibrary loans and prevent professors from using such materials as part of their courses.[22]

The concerns of the civilian educational institutions are echoed at Air University. Though a military organization, Air University is similar to other educational bodies in that it is also concerned with "intellectual property" access and vulnerability. As part of research, students often require the use of copyrighted materials, yet the Research Survey discovered that military students consider copyright issues to be a low concern (see appendix D). Does Air University's obligation to protect that material change by the fact that the research papers are going to be available on-line? After consulting with legal experts, Air University adjusted the copyright releasability form to include a notice that the information was going to be electronically released and available on the Air University Web server.[23]

Outside of the academic arena, the Air Force has other information distribution concerns, namely that of "releasability." There are already procedures set in place through AFI 35-205, *Air Force Security and Policy Review Program*, to provide expert review of the information before it is publicly released.[24] Local area networks (LAN) and the routine use of e-mail have revolutionized communications within and among military installations; however, even closer to the heart of the issue is the internet's direct

interface with private sectors (domestic and foreign). The Air Force's requirement for public affairs and security reviews challenges Air University: it simultaneously seeks open exchange with outside agencies, while striving to protect DOD interests regarding defense-related information.[25]

Additionally, "releasability" could apply to the transmission of "organizational e-mail," as described in AFMAN 37-126, *Preparing Official Communications.* The manual recommends an organizational e-mail account to control the release of information from an office and ensure unified organizational communications.[26]

Proposed Policy

The Air Force must deal with the challenges of copyright and releasability. The only viable, over-arching solution seems to be *training* (see also "User Training," page 51). As a publishing executive said with regard to the French copyright incident discussed above, "just as we teach our children not to steal toys, just as we teach our children not to plagiarize, we have to get across the message that you don't steal from the Internet."[27] Within the Air Force, members must learn, and understand the importance of respecting, copyright restrictions. Additionally, releasability requirements, including lessons on Air Force policy, must be stressed. Each organization should have an e-mail account to ensure that messages are properly coordinated and released from the appropriate level.

Recommendation

Incorporate the lessons in user training that copyright protection rules protect intellectual property creators and the Air Force alike. Review public affairs and security

requirements for information releasable on the Web. Set up organizational accounts to ensure each unit speaks with "one voice."

Official Use

Most official government publications do not define the term "official use." Many publications liberally use the term "official business" or "for official use only," but it is often difficult to define these phrases, especially with respect to something as new as internet policy. Users need these definitions, however. A user needs to know the legitimate bounds within which he or she can use the new technology.

Existing Policy

Air Force publications do not clearly define "official business," as it relates to the internet. Air Force Materiel Command (AFMC) Instruction 37-102, *Transmission of Information via the Internet*, states that using government-provided resources (hardware and software) for nonofficial business is prohibited. It does state that commanders can authorize personnel to use the government resources to further their military or professional knowledge, but only during non-duty hours.[28] It is probably better to view this guidance with the definition of "official use" as what is and is not allowed and "authorized use" as what can be *additionally* authorized by commanders.

"Interim Internet Guidance" (draft) from Headquarters USAF has prohibitions similar to AFMCI 37-102. The guidance dictates that administrative, non-judicial, or judicial punishment may be imposed for using the internet for non-official purposes. It states that commanders and supervisors are responsible for ensuring assigned personnel use the government equipment and services for official use only and for determining what

activities will be authorized for their organization. Like AFMCI 37-102, the guidance gives the commander authority to allow personnel to use government resources to further their professional and/or military knowledge during non-duty hours. The guidance allows that any legal and ethical use that is in the best interest of the Air Force may be authorized. However, the only thing that is *specifically* detailed is that "government-owned equipment will not be used to access commercial internet services or fee-for-use services unless for official business."[29]

The guidance provides no other specific details and no details on what activities are in the best interest of the Air Force or what is considered official use. Certainly, this last mentioned restriction was intended to stop personnel from using government resources to connect with personal ISPs. However, the wording of the guidance is vague enough to also include restrictions to connecting to free, commercial news services such as CNN Interactive[30] which is a perfectly legitimate source of information for the Air Force professional. Whatever the intent of the guidance; it is not unambiguous, it has potential for actually *reducing* productivity of the user, and sorting through the various guidelines from the multiple commands is certainly confusing.

Because communicating on the internet is so new to most Air Force personnel, a parallel can be drawn with a government-provided resource that is better understood—the *telephone*. The *Joint Ethics Regulation* (JER) states that the use of the federal government telephone system "shall be limited to conduct official business. Such official business calls may include emergency calls and calls that the DOD Components determine are necessary in the interest of the Federal Government." The JER goes on to define calls that are "in the interest of the Federal Government" as being "personal calls

(such as calls to speak to a spouse or minor children or to arrange for emergency repairs to residence or automobile) that must be made during working hours" as long as these calls are consistent with the following criteria: [31]

1. Calls must not adversely affect the performance of the official duties of the employee or organization;
2. Must be of reasonable duration and frequency;
3. Could not reasonably have been made at another time;
4. Long distance calls are not charged to Federal Government or are 800 toll free;
5. And when traveling for more than one night on TDY within the United States, a brief call to his residence to notify family of schedule change.

Another official use issue is the *accessibility* of internet sites (for example, Web sites or home pages). Because of the openness of the internet there are many sites that specialize in pornographic, "hate" material, or hacker and cracker information. Obviously, these sites contain little information pertinent to official or personal business sanctioned by the Air Force. Private organizations are already addressing this problem. A company called Webster Network Strategies of Naples, Florida builds electronic "filters" into office networks that prevent workers from using the internet for accessing "disallowed" sites. This "filter" program has already been sold to such big customers as Boeing Co., Northeast Utilities, and the Florida Department of Transportation.[32] Another program, SmartAlex begins "photographing" the computer's screen at regular intervals when it detects internet activity. Text is automatically searched for up to nine categories of offensive content: "sex" and "intent to commit crime" are but two. The program attempts to categorize each graphic as either "normal" or "possessing suspicious characteristics" based upon such things as flesh tone content and color distribution. Additionally, the software leaves a trail to indicate to the network administrators if any attempt has been made to bypass it.[33]

The Air Force has not made a high-level universal decision whether these pornographic, "hate" material, or hacker and cracker sites should be "disallowed" by restricting access. If these sites are restricted, the Air Force must decide if it will actually prevent access to the sites or just mandate avoidance of the sites.

Proposed Policy

As communication technology increases, more unclassified official business will be conducted on the internet and particularly the Web. In addition to official business, more "everyday" personal items will be conducted on the Web, as well. An appropriate analogy may be when the telephone was first made common, more and more official *and* personal business came to rely on the telephone. Now the telephone is so common in the office environment, business would come to a standstill if it were not available. Personnel would have to take time off from work to either take care of the personal business or go to a location that had a telephone to take care of the personal business. This is why the JER specifically allows personnel the use of a government-provided telephone.

Similarly with the internet, as more and more personal and official business becomes dependent on the internet, workers will need to access e-mail, FTP sites, and Web home pages just as workers now need to call the realtor, mechanic, or spouse. Obviously, this need to access the internet during work hours goes beyond the explicit direction in AFMCI 37-102 and the Air Staff "Interim Internet Guidance" which states that nonofficial use could be authorized by commanders, but only during non-duty hours to further their professional or military knowledge. The author of the AFMC Instruction has stated that his intent was to define communication via the internet as the same as

communication via the telephone.[34] In other words, when the JER states that "official business calls may include emergency calls and calls . . . [that] are necessary in the interest of the Federal Government,"[35] it implies that official business *communications* (to include telephone calls, e-mail, faxes, and other electronic communications) may include emergency communications and communications that are necessary in the interest of the federal government. The author of the AFMC Instruction has stated that he has approval from the HQ AFMC legal office (AFMC/JA) to make this interpretation.[36] However, what is and what is not allowed with respect to use of government-provided communication resources still needs to be clarified. When AFMCI 37-102 is interpreted as the author intended, there is still inconsistency. For example, one of the "specifically-prohibited" activities from this instruction is the personal use of e-mail and internet for nongovernmental purposes.[37] This prohibition is obviously in conflict with the intent to use the internet, like the telephone, to increase productivity even if this means conducting some personal business.

New policy should recognize the internet as merely a tool (albeit a *new and powerful* tool). Tools can be used to perform official business, as well as personal business. If the tool makes the worker more productive because less time is spent on personal business, then supervisors should be tolerant on the use of the internet for personal business during duty hours. The specific prohibition in the Air Staff "Interim Internet Guidance" from using government equipment to access commercial internet providers would keep Air Force users from checking their personal e-mail accounts from their work station.[38] There are numerous examples of why it may be more efficient for a user to retrieve or send personal e-mail from work. The user may be waiting for a response from a realtor

from his/her next duty station or important e-mail from his/her spouse. Checking personal e-mail from work would be analogous to calling home on the telephone and checking the answering machine.

Another use of the internet that the reviewed guidelines explicitly do not allow is nonofficial use during duty hours to increase professional knowledge. But is it nonofficial use for a person to spend a reasonable amount of time using the technology so that she can learn to exploit it to make herself even more productive? No one balks at personnel taking courses during duty hours to improve productivity using a word processor or time management. Just because the potential exists for abuse of the technology does not mean that the technology should not be exploited to its fullest.

Personal use of the government resources must of reasonable amount. However, it is easy to abuse the technology. A company which sells "filter" software to companies to prevent users from visiting certain sites has found that workers at some companies average 90 minutes a day accessing erotic sites, sports news, and others.[39] Another company sells software that actually scans the computer display looking for "disallowed" subjects to prevent "unchecked personal use of the internet" to reduce unproductive employee time and reduce computer disk space and capacity that is being "eaten up quickly by inherently large images that are downloaded by Web-browsing employees."[40]

In addition to allowing reasonable amount of personal use, the Air Force must decide whether "disallowed" sites will be restricted and if so, how. This is an ongoing issue within the Air Force that has gotten increasing attention. The AFIN Program Management Office has begun addressing the subject.[41] Lists could be generated of these sites and firewalls could be programmed to not allow access to these sites. Several

questions arise here, however. Who has the authority to generate and implement this list? Is it an Air Force-wide list? Is it maintained by local network administrators or local commanders? If a site is not on the list, is it by definition "allowed?" Another approach is to direct personnel, or users, not to access these sites or these *types* of sites. Programming firewalls to disallow a specific list of sites should not be done. Beyond the censorship issue, which is not necessarily an issue in the military, the mechanics of maintaining this list would be prohibitive. The internet is growing and evolving so rapidly that any list of "disallowed" sites would be out of date before it was even published. A training, rather than a technical, solution is the practical answer. Users must be trained on which sites should not be visited on government time or with government resources (see also "Data Download," page 43).

The previous discussion points to the need for a policy that is specific to personnel and users as to the definition of official use. A good working definition would be based on what was is the best *overall* interest of the federal government. "Official use" should include normal work-related internet use and a reasonable amount of internet use to increase professional knowledge on how best to exploit the medium.

This must be balanced by a good definition of authorized use. Here, a good working definition, with respect to the internet and electronic communications, would be similar to that of the telephone. "Authorized use" should include a reasonable amount of personal use: to include emergency communications, communication to family members while the member is traveling on official business, and normal personal communications such as a prudent amount of e-mail, real estate downloads, and communications with an auto or home repair service. The definition of "reasonable" remains ambiguous.

However, there are no strict time limits for personal use of the telephone and commanders often manage to maintain order and discipline personnel that abuse this privilege. The definition of reasonable use aside, the official guidelines must be specific enough to let the user know, *without* explicit direction from the local commander, what personal use is authorized. On the other hand, the guidelines must not be so restrictive, as they are today, that they limit the ability of Air Force personnel to learn how to exploit the technology to its fullest.

Recommendation

New guidelines should define official use as what is in the best *overall* interest of the federal government. This should include normal work related internet use and a reasonable amount of internet use to increase professional knowledge on how best to exploit the medium.

New guidelines should also define authorized use so that internet and electronic communications, are viewed similarly to that of the telephone. This should include a reasonable amount of personal use: to include emergency communications; communication to family members while the member is traveling on official business; and normal personal communications such as a prudent amount of e-mail, real estate downloads, and communications with an auto or home repair service.

It should incorporate the concept that communications during duty hours, whether it is via telephone or via the internet, must allow for *reasonable* use for personal business. Just as in the telephone today, the local commander will always retain jurisdiction on defining the limits of reasonable use.

Additionally, Air Staff should provide guidance to prevent local administrators or commanders from generating lists of "disallowed" sites, but rather train individual users which type of sites not to access.

Finally, equating communication via telephone with communication via internet must be explicitly made within the guidelines until such time use of the internet is as common as use of the telephone.

Data Download

Current Situation

There are a number of ways to transfer data. The easiest and most popular services or protocols are FTP and HTTP (hypertext transfer protocol, used by the Web). Very little policy or guidance exists on what *specifically* can be downloaded or transferred across the internet. Most publications concentrate on categories of information that should not be downloaded.

For the purposes described here, official use data transfer is that which is required for the *efficient* performance of the user's job (see also "Official Use," page 35). Some examples of "official use" are Air University students downloading research material, or a squadron member downloading the Pentagon's "Earlybird" for the unit. Some obvious examples of downloads that are not "official use" are downloading stock market information, personal software, or of course, pornographic material. There are several publications and policies that list appropriate material to download. The *Air University Guidelines for Computer and Information Systems (draft)* and the new AFMCI 37-102, *Transmission of Information via the Internet* lists "offensive or obscene material, such as

pornography or hate literature" as inappropriate.[42] The *Air University Guidelines* also list inappropriate activities as those that seriously interfere with other, legitimate users. Example activities include "hogging" systems for non-official purposes (for example, game playing) and excessive large file transfers.[43]

AFMCI 37-102 also explicitly discusses downloading files. In this discussion, users are warned to protect against computer viruses by virus-checking all files downloaded, including files attached to e-mail messages. The instruction states:

> the Air Force prohibits the use of software acquired directly from non-DOD electronic bulletin boards, the public domain, or shareware sources. The Air Force allows the use of public domain or shareware software only after it is certified by a software testing facility, such as the Air Force Information Warfare Center (AFIWC); the Standard Systems Group, Hill AFB UT; or the Standard Systems Group at Maxwell AFB–Gunter Annex, AL (AFI 33-114, *Software Management*).[44]

In February 1996, guidance was given at Kelly AFB, Texas to prohibit users from using Java-enabled browser software.[45] Java is a programming language that makes it possible to run small applications remotely over a network, obviating the need for application software residing on the local hard drive.[46] Although the message giving this moratorium does not specifically address visiting Java sites, it does prohibit using software that could download Java applets (see additional discussion in appendix B). No rationale for this moratorium was included, but one could assume that the concern was that Java applets are essentially executable files that are downloaded but have not been virus-checked nor certified by the appropriate USAF organizations.

Proposed Policy

The above discussion on existing policy implies several broad categories of inappropriate download activities. The first category, offensive or obscene material, is

obvious and indeed is included in nearly every policy or guidance available for military or business use of the internet.

The second category is excessively large files or activities that take up large amounts of system bandwidth. Every computer network, regardless of the level of technology involved, has a maximum amount of bandwidth available. This bandwidth must be shared by all of the users. An analogy may be to compare the LAN capacity with a large diameter water pipe. If there are a small number of users requesting a small amount of water apiece from the pipe, they will probably all get the water flow that they requested. If there are very many users requesting a small amount of water apiece, there may not be enough capacity in the pipe to provide for all of the users. And finally, if one of the water users demands an unusually high amount of water flow, the other water users will be severely limited. Likewise in a computer network, if one user demands a large percent of the system bandwidth to download a large personal file, some of the other users may be faced with degraded system performance for some time. Obviously, as technology increases so too does the typical bandwidth of computer networks, however, so too does the size of the typical file.

The third category is material that does not contribute to official business. For defense of this, the JER is used again. The JER was referenced in the section above on "official business" (see page 36). In that section, official business with respect to government-provided communication resources was defined to include a *reasonable* amount of use for personal business. Downloads should have the same definition. An Air Force member may be looking for a new job in anticipation of a permanent change of station (PCS) and download a fairly large file containing job listings from the Air Force

Personnel Center (AFPC), or the member may download a listing of available real-estate at his next duty location. There are many examples of legitimate personal downloads that fall within the definition of the proposed expanded interpretation of the JER.

The last prohibited activity is downloading software from non-DOD sites, public domain sites, and shareware sources before it has been certified by an approved software testing facility. Although this prohibition is entirely appropriate, it often leads to violations merely because the user does not know that the rule exists or the user is intimidated by the official procedures required to certify software. Streamlined procedures need to be established to make this task of requesting certification easier for the user and still allow a quick turnaround time back to the user.

Finally, although not a specific prohibition to downloads, files that are downloaded, including attached files to e-mail messages, must be virusvirus" checked before permanently installing on a user's hard drive or on the system network. Many users, however, do not have appropriate anti-virus software, and much of the anti-virus software is not set up to check files automatically as they are downloaded. Every computer system that is capable of downloading files should have automatic virus checking software installed, and the anti-virus software must be updated frequently to include recent virus profiles.

The issue of prohibiting Java is a valid concern. Although Java has been designed as virusvirus" resistant, there is still concern about security "holes" within Java.[47] Java technology is advancing rapidly and these "holes" should be "patched" soon. New features, such as Java, must be addressed quickly by network security personnel, and Air Force-wide guidance must be rapidly disseminated to users on how to use new features.

Recommendation

Air Force policy should stress four main categories of inappropriate downloads: offensive or obscene material, excessively large files that take up large amounts of system bandwidth, non-official business, and non-certified software. Additionally, computers that are capable of downloading files must have automatic virus-checking software installed. This software must be updated frequently and automatically by the LAN administrator. Software testing facilities must quickly address new features on the Web and the remainder of the internet to provide input to policy makers. New policy must be written and disseminated to users.

User Security

Duane Edwards commented on security in Toffler's *War and Anti War*:

> Our information security is atrocious, our operational [secrecy] is atrocious, our communications security is atrocious.[48]

Recent surveys, including one from the University of Michigan Business School, corroborated this project's Research Survey that security is the number one concern of internet users.[49] The rapid increase in technology has made internet communications more and more secure. However, a common security axiom is appropriate: "information is only as secure as the people using it." The system may have incredible software and hardware security protection, but potentially, one naïve user can "crash" a system or open a system to outside "attack." The physical system may be secure, but if the people are not security conscious as well, the overall system is still weak.

Responsibility for operational security (OPSEC) and communications security (COMSEC) ultimately rests with the individual. An infamous example of an individual

violating both OPSEC and COMSEC via the internet can be found in the case of the rescue of Capt Scott O'Grady. The wingman to the pilot who first made contact with Capt O'Grady after O'Grady was shot down in Bosnia wrote an e-mail which he sent to some of his friends on the internet. These friends in turn "forwarded" the e-mail to their friends and so forth. The original e-mail was certainly written with good intentions, but clearly violated the spirit of both OPSEC and COMSEC. Even though the e-mail was written in 1995, a full-text version can still be found on the internet.[50] Using a common "search engine" with the keywords "Scott O'Grady," the site can be uncovered within a few seconds.

In addition to improper use by authorized users, e-mail presents other security problems. E-mail is stored on a central server and the server maintains individual user accounts that are protected from one another. It is possible for a "cracker" (a malicious hacker) to gain access to the server and therefore all e-mail accounts. Although conventional e-mail should not contain classified information, there are many unclassified uses of e-mail and other data transfers that contain sensitive or personal information. A good example is an individual who transmits his name and social security numbers to AFPC as a volunteer for a job that is listed on the "Assignments Online" bulletin board.[51] While the e-mail or data transfer is intended only for the AFPC assignment team, it is conceivable a cracker could intercept a sensitive message or gain access to AFPC accounts. Air Force e-mail users should have some assurance that their personal information and other sensitive information is secure.

In many ways, internet security breaches are similar to a security breach caused by lax phone discipline. Both the internet and the phone carry electronic messages, and it is

incumbent upon the sender to ensure that the message is proper and unclassified. The major difference is that an internet message, or an e-mail, is a permanent record that *can* receive worldwide distribution once it is sent. Phone calls, typically, are not recorded and replayed for anyone who wants to listen. Using the above e-mail example, the originator may not have thought twice about saying all of the disclosed information to a friend over the telephone (although he should have), but it is not hard to second guess if he would have called up thousands of perfect strangers and told them the same thing over the phone.

Current Situation

Numerous official publications exist to provide direction to users on security. In fact, of the 36 official publications reviewed for this study, more than half were specifically pertinent to security (see chapter 2). Several of these publications reference other documents or have MAJCOM supplements. Many of these guidelines contained valuable security information; however, sorting through the myriad of documents is daunting for the typical user. As a result, most people do not know the contents of these instructions and the information contained within is lost. For example, the simple act of changing passwords often, to something that is not easy to guess, goes a long way to enhancing security. However, unless the user finds this reference in one of the numerous guidelines, he may not know of the requirement and as a result may leave a hole that would have been simple to plug.

A recognized internet expert at ACSC, CDR Homer Coffman thought the biggest security risk is lack of knowledge. In his experience working in the Technology Division of ACSC, security problems come from users who do not understand the technology and

accidentally do something or allow something to happen.[52] No organized Air Force or DOD directive exists mandating training for users. With the vast number of computer users, it would be hard to implement an all encompassing training program. Many organizations have their own user training programs. ACSC has made a definite effort to provide computer training and internet education to students. A 1995 ACSC research project outlined an entire course for new users of the internet.[53]

Proposed Policy

From the above discussion, it can be seen that two user security concerns are the need for centralized guidance and the need for user training and knowledge.

Many existing official publications provide direction to users in security matters such as password protection, OPSEC, and COMSEC responsibilities. Even though these numerous publications do not typically conflict with each other, the very fact that there are so many publications makes it difficult for users to grasp the nature of the internet policy with regards to security. A centralized set of policy publications governing user security would help the situation.

In addition to guidance, the user's knowledge base must be increased through training. Technology advances in hardware and software have greatly enhanced the security of computer and LAN systems, but the system is only as secure as the person operating it. There are numerous relatively easy precautions that users can take to greatly enhance the security of their computer and of their LAN. They can do simple things like shut down their computer when they step away from it, or use software "locks" and passwords, change their password often and use non-descriptive passwords. The main issue is that users are often not *aware* that they can or should do these things or may not

understand the ramifications if these precautions are not taken. Regardless of their personnel's level of awareness, unit commanders should still ensure that proper computer security practices are followed.

One aspect of technology that users can implement is simple encryption. One potential encryption software candidate is Pretty Good Privacy (PGP).[54] PGP is a dual key encryption methodology that is widely available. PGP users have a publicly-available key and a private key. The sender uses the receiver's public key to encrypt the message and the receiver decrypts the message using his private key. While PGP may not be suitable for classified information, it is suitable for transmitting sensitive personal information.

Recommendation

Establish a centralized publication that specifically addresses user security issues. This centralized publication should be integrated into the capstone internet policy. Centralized guidance should be provided to individual organizations on suggestions for training courses for users. Unit commanders have the responsibility of ensuring compliance with proper computer security practices. The Air Force should consider implementing protection techniques, such as simple and available encrypting, for unclassified, yet sensitive, e-mails and data transfers.

User Training

The internet is a relatively new phenomena to most Air Force personnel. Unless they have personal computers with home internet access, Air Force personnel are probably not comfortable with the new technology. The results of the Research Survey indicate that a

vast majority of officers own computers (93 percent), but only 65 percent have private internet access. Correspondingly, 76 percent of the surveyed enlisted corps own computers and only 24 percent of them had internet access at home. Even when personnel have and use a computer at home, it is difficult for them to get up-to-date information and training on their own. In fact, the Research Survey found that user training is a significant concern. It is extremely important for users to understand the technology so they can best exploit it.

Current Situation

The issue of users not having sufficient knowledge or training has manifested itself throughout the topics addressed within this research. Lack of user knowledge is a *common* ingredient to every issue specific to "User Policy Analysis" (chapter 3) in this research. Without training, users have no basis to understand fundamental e-mail "netiquette" (see "Individual Communications," page 20). Users sometimes unknowingly violate other users' privacy by forwarding embarrassing e-mail messages (see "Privacy," page 23). Some users do not understand the ease with which delicate decency and harassment subjects can be violated with instantaneous and impersonal digital communications (see "Cultural Issues," page 28). Similarly, Air Force personnel do not understand the implications of protecting copyrights and controlling the releasability of information (see "Copyrights and Releasability," page 30). The Research Survey results indicate that Air Force officers ranked copyright protection as their lowest priority of the surveyed issues.

Additional confusion is created when inconsistent guidance is provided concerning what is and what is not allowable or considered official use on the internet. Most Air

Force personnel would not balk at taking a reasonable number of personal telephone calls at work, but users have no way of knowing if they are allowed to send and receive a reasonable number of personal e-mails at work (see "Official Use," page 35). Finally, most users are firm believers of the importance of security. In fact, the Research Survey shows that overall, the respondents thought that security was the most important internet issue. However, the officers surveyed thought that security was considerably more important than did the civilians. Without training, users are prone to make mistakes that have costly security implications (see "User Security," page 47).

There is no Air Force-wide standard for training personnel on use of the computer, let alone on the particularly application of internet use. Many organizations have training available. A 1995 ACSC research project outlined an entire course for new internet users and has begun limited classroom training.[55] Other organizations have begun putting training and internet tutorials on-line, available across the internet.[56]

Proposed Solution

Mandating training for every internet user in the Air Force is too extreme. Individual internet knowledge covers the entire spectrum among personnel. Some users already have sufficient knowledge in many areas and only need training on specific subjects. Other users may be very new to the internet technology and are intimidated without training. These new users need to be "pulled" into the technology and shown that it is relatively easy to use and can be exploited to greatly enhance the mission. Because of vast differences in internet proficiency of personnel and the different application of the technology to different units' missions, Air Force- and MAJCOM-wide *required* training is too excessive. Individual organizations should make training available to internet

users, and the organizations must determine the type and level of training that will be made available. For example, although an Air Force Survival School might use the internet for e-mail and other applications, because of the "low-tech" nature of its mission, it probably will not have the same internet intensive requirements of other organizations such as Air University, which conducts a significant amount of research and study on-line.

Recommendation

Individual organizations should provide flexible internet training to personnel dependent upon the degree of user proficiency and mission requirements. Organizations should encourage personnel to take advantage of the training to familiarize themselves with common applications, user etiquette, and security awareness. This will allow users to know better how to exploit the new technology to enhance the mission.

Notes

[1]Arlene H. Rinaldi. (1995). *The Net: User Guidelines and Netiquette* [On-line]. Available HTTP http://www.fau.edu/rinaldi/netiquette.html [1996, March 26].

[2]Isaac Asimov. Introduction to *Isaac Asimov's Robot City: Odyssey* by Michael P. Kube-McDowell (New York: Ace Books, 1987), x.

[3]Privacy, Invasion of. (1993). *New Grolier Multimedia Encyclopedia*, (Release 6), [CD-ROM], 3.

[4]Robert Hauptman and Susan Motin, "The Internet, cyberethics, and virtual morality," *Online,* March 1994, 8.

[5]Jon Chesnut, Ph.D. (jdchesnut@invitrogen.com). (1996, February). Invitrogen's E-mail policy. E-mail to Maj Scott Chesnut (71042.664 @compuserve.com).

[6]Chris Bucholtz, "Mind your manners," *Communications International,* May 1995, 8.

[7]Hauptman and Motin, 8.

[8]Bucholtz, 9.

[9]AFPAM 36-2705, *Discrimination and Sexual Harassment*, 28 February 1995.

[10]Brad Templeton. (1994). "10 Big Myths about Copyright Explained," Myth 1. [On-line]. Available HTTP: http://www.clari.net/brad/copymyths.html [1996, February 21].

Notes

[11]Discussion on *Star Trek: Generations* [On-line]. Available UseNet: alt.startrek.creative [August 94].

[12]"The Air University Homepage." [On-line]. Available HTTP: http://www.au.af.mil/ [25 Mar 96].

[13]Templeton.

[14]HKK. (1995, February 14). Dennis Erlich Rumors. "Discussion on the Erlich Case." [On-line]. Available HTTP: http://www.eff.org/pub/Legal/Cases/CoS_v_the_Net/cos_raids_ erlich_021495.statement [1996, March 20].

[15]Jim Connelly, "Royal Stings," *websight,* issue 1, 14-15.

[16]Edmund F. Scherr. (1995, September 5). "U.S. Outlines Safeguards for Intellectual Property Rights". [On-line]. Available HTTP: http://sunsite.nus.sg/usis/New/Update/090595.html [1996, February 6].

[17]"French Book Banned, Then Pirated." (*New York Times,* 18 March 1996, A1). [On-line]. Available via Edupage List: listproc@elanor.oit.unc.edu [1996, March 20].

[18]"International Copyright Conference." (*Financial Times,* 14 February 1996, p7). [Online]. Available via Edupage List: listproc@elanor.oit.unc.edu [1996, February 18].

[19]Templeton, Myth 1.

[20]"The Report of the Working Group on Intellectual Property Rights." (1995). [Online]. Available HTTP: http://www.uspto.gov/web/ipnii/ [1996, March 20].

[21]"The Report of the Working Group on Intellectual Property Rights."

[22]"Higher Ed Groups Eye Electronic Copyright Bill." *(Chronicle of Higher Education*, 16 February 1996, A26). [Online]. Available via Edupage List: listproc@elanor.oit.unc.edu [1996, February 18].

[23]Col Charles White, memorandum for record, subject: AU Copyright Conference, 27 July 1995.

[24]AFI 35-205, *Air Force Security and Policy Review Program*, 25 February 1994.

[25]AU/RCO. *Synopsis of Written Guidance Concerning the Release of Information via Internet,* no date.

[26]AFMAN 37-126, *Preparing Official Communications*, 10 February 1995.

[27]"French Book Banned, Then Pirated."

[28]AFMCI 37-102, *Transmission of Information via the Internet.* [On-line], para 2.Available HTTP: http://www.afmc.wpafb.mil:12000/publications/AFMC_Instructions/37-102.doc [1996, February 21].

[29]Col Miller AF/SCXX (millerb@afsync.hq.af.mil) (1996, February 28). Interim Internet Guidance. E-mail to Maj Matonak (amatonak@max1.au.af.mil).

[30]"CNN Interactive." [On-line]. Available HTTP: http://www.cnn.com [1996, February 9].

[31]DOD5500.7-R, *Joint Ethics Regulation*, August 1993, Secretary of Defense, para 2-301.

[32]Marc Gunther, "Goofing off at the office goes high-tech." *Montgomery Advertiser*, 24 March 1996, 8F.

Notes

[33]"Parental Control Software Effectively Monitors Employee's Internet Activity—Improves Productivity" (26 March 1996). *PR Newswire*. [On-line via PointCast Network]. Available HTTP: http://pcn.com [1996, March 26].

[34]Maj Phil McDowell (mcdowep@WPGATE1.wpafb.af.mil). (1996, February 28). re: more internet questions. E-mail to Maj Jon Link (jlink@max1.au.af.mil).

[35]*Joint Ethics Regulation*, para 2-301.

[36]McDowell. (1996, February 28). re: more internet questions.

[37]AFMCI 37-102, para 2.

[38]Miller.

[39]Marc Gunther, 8F.

[40]"Parental Control Software Effectively Monitors Employee's Internet Activity—Improves Productivity."

[41]Darrel Beach, DDN Program Management Office, interview with Maj Matonak, 14 February 96.

[42]AFMCI 37-102.

[43]*Air University Guidelines for Computer and Information Systems (draft)*, 24 October 1995.

[44]AFMCI 37-102, para 7.1.3.

[45]Kris Krimmel (kkrimmel@sagate1.kelly.af.mil). (1996, February 28). Applet Enabled Browser Moratorium Issued at Kelly. E-mail to Multiple recipients of list <www@infosphere.safb.af.mil>.

[46]Robert Hertzbert, "Java Picks Up Steam," *WebWeek* 2, Issue 1, Jan 96.

[47]James Kim, "Security flaw found in new Netscape software," *USA Today,* 22 February 1996, B1.

[48]Alvin and Heidi Toffler, *War and Anti-War* (New York: Warner Books, 1995), 176.

[49]"Consumer Survey of WWW Users, Preliminary Results from 4th Survey." (12 December 1995). University of Michigan Business School. [On-line]. Available HTTP: http://www.www.cc.gatech.edu/gvu/user_surveys/survey-04-1995 [1995, December 20].

[50]Mike Howells. (no date). *"EJECT! EJECT! EJECT!" (full transcript of e-mail written by Scott Zobrist, wingman of pilot who first made contact with downed F-16 pilot Scott O'Grady in Bosnia, original e-mail date 8 June 1995)*, [On-line]. Available HTTP: http://www.i1.net/~mhowells/eject.html [1996, March 10].

[51]"Assignments Online" Available HTTP: http://www.afpc.af.mil/asgnment/htdocs/ [1996, March 18].

[52]CDR Homer Coffman, ACSC DT, Maxwell AFB AL, interview with Maj Jon Link, 7 February 1996.

[53]Maj Richard Carroll, et al., *Internet: Education and Application for the Knowledge Warrior*, ACSC/DEC/045/95-05, Maxwell AFB, Montgomery, AL: Air Command and Staff College, May 1995.

[54]Jeffrey I. Schiller. "MIT Distribution Site for PGP." (1995). [On-line]. Available HTTP: http://web.mit.edu/network/pgp.html [1996, March 26].

[55]Carroll.

Notes

[56]Mr. Charles Hall, Systems Engineer, Silicon Graphics Corporation. Briefing to ACSC Students, 13 December 1995.

Chapter 4

Administrator Policy Analysis

This chapter continues the ascent up the "Internet Policy Pyramid" (figure 1-3) by addressing the middlemen of the internet community: the network administrators. The explosive popularity of the Web highlights the difficulties facing network administration: better, newer products will continue to need more processing speed, more hard disk space, and more bandwidth (additional discussion on "bandwidth" in "Data Download," page 43) to run over the internet. Lack of network performance, particularly performance with regard to bandwidth, hampers the user's ability to exploit the medium. This was a major complaint among Research Survey respondents. Computer technology appears to be proceeding at a pace creating a new generation of computer hardware every twelve to eighteen months.[1]

This chapter addresses the challenges that implementing new technologies are causing Air Force network administrators. Since two distinctly different communities are involved in Air Force network program management, this chapter addresses the challenges to the "long-haul" networks and "local" networks separately. This chapter also addresses specific network administration issues such as training, Web site standardization, access privileges, and security.

Long-Haul Networks Capacity

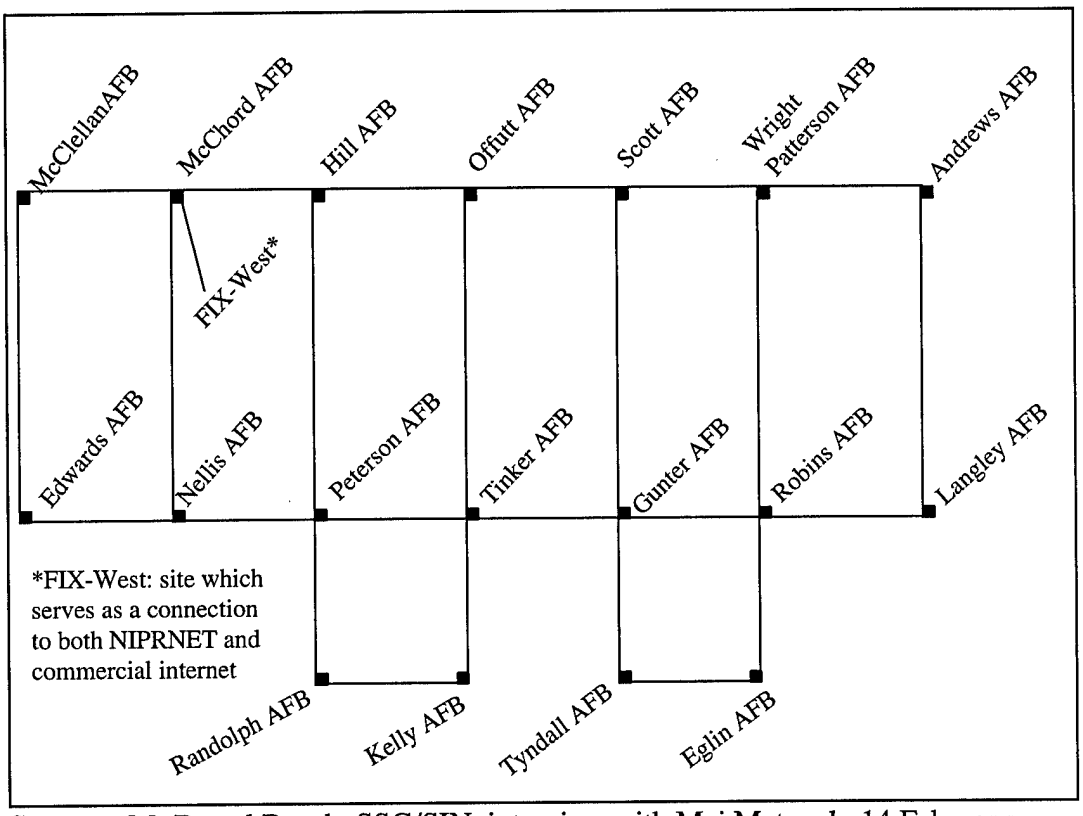
Air Force networks may be broken down into the two general areas of long-haul trunk lines and the base-level LAN. Long-haul connectivity is normally provided via the Air Force Internet (AFIN). The AFIN is a network of circuits managed and funded by the Air Force. It connects to the larger DOD Non-secure IP Router Network (NIPRNET) via just two "gateways."[2]

Current Situation

With Web and other long haul internet applications "eating" available bandwidth, the AFIN and its gateways to other internet "networks" are beginning to feel the strain. In an effort to ease that strain, long-haul commercial telecommunications suppliers are working hard to implement higher capacity Integrated Switched Distributed Network (ISDN) lines. The telecommunications bill[3] passed by Congress in early 1996 will go further by encouraging the implementation of Asynchronous Transfer Mode (ATM) circuits. ISDN and ATM technologies will help connectivity within the AFIN. However, bottlenecks at the AFIN to NIPRNET will remain until additional gateways are provided.

Proposed Policy

To improve NIPRNET connectivity for its bases, the AFIN program office is working with the Defense Information Systems Agency (DISA) to provide direct NIPRNET connections for all bases by Fiscal Year 1997 (FY97).[4] In addition, the AFIN program office has programmed an increase to the connectivity between "core" Air Force bases (figure 4-1) by FY97.



Source: Mr Darrel Beach, SSG/SIN, interview with Maj Matonak, 14 February 1996.

Figure 4-1. Proposed Air Force Internet Network Connectivity Topology

By using a single point of access for both circuits, the Base Network Control Center (BNCC) will be able to expand the circuits most needed for their base's missions. The BNCC concept is designed to be the single focal point on each base for providing network management and customer support to critical services.[5] For those few customers who need extensive connectivity to the worldwide commercial internet, projects such as Barrier Reef[6] (see "Administrator Security," page 82) may allow these customers access to commercial internet connectivity without compromising security and service for the remaining base customers. The AFIN program office is already prepared to address customers who feel connectivity to commercial internet is needed to meet their mission requirements.[7]

Recommendations

For Web users to see adequate response times, good connectivity to the rest of the DOD community is essential. The Air Staff needs to support and implement the funding and programs necessary to eliminate the need for NIPRNET gateways as well as to increase the bandwidth between core Air Force bases.

Base-Level Capacity

This section addresses the "local" or base-level capacity and bandwidth challenges. The base-level challenges are similar to the long-haul bandwidth challenges faced by AFIN.

Existing Situation

At the local or base-level, the bandwidth challenges and potential bottlenecks mentioned in the previous section become more acute. Depending on how effectively a Web page designer puts together the graphics, and what user preferences are set, Web programs have the capacity to bring standard base networks "to their knees." As the Web becomes more and more popular, not only as a browser but also as an interface "front end" for telnet and file transfers, a normal base LAN is going to need more than just increased bandwidth on its external internet circuit. It will also need greater throughput on its local routers (equipment that forwards packets of information along the path), and greater bandwidth on each individual LAN.

To better understand the situation, consider the typical base LAN (figure 4-2) and its bandwidth. On most bases, the LAN is a collection of loosely-joined subnets that may or may not tie to the BNCC, or rather a central base LAN. This is because the computer

network physical infrastructure (the cables, routers, concentrators, ethernet hubs, etc.) has historically been the property of the individual organizations.

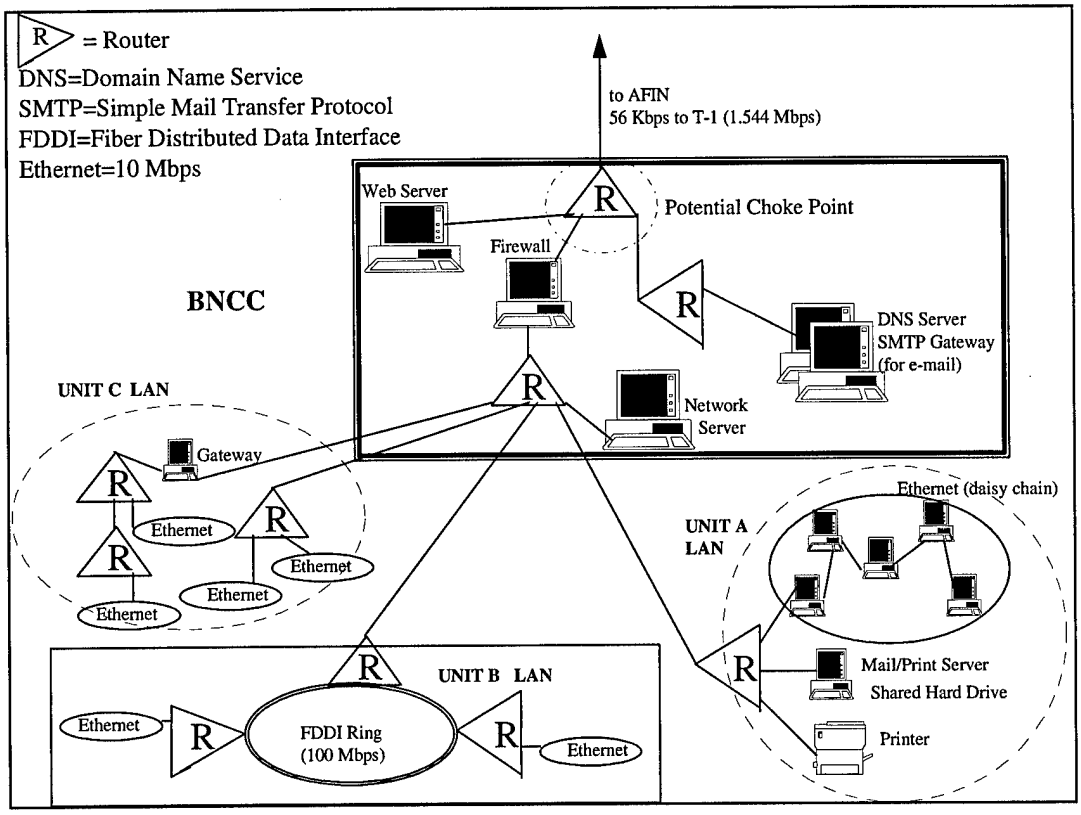


Figure 4-2. Typical Base Local Area Network (LAN)

The "choke" points become apparent. Four to eight ethernet standard connections (each at 10 megabits per second (Mbps)) trying to squeeze through one 10 Mbps ethernet router and finally to a base AFIN circuit that could be as "narrow" as "T-1" standard (.56 to 1.544 Mbps). This "choking" of bandwidth creates some challenges. Unlike e-mail, in which messages can be stored at mail servers until the circuit is free, with the Web, a user must wait his turn in line to get a piece of that circuit.

Proposed Solution

The solution to the local-level problem centers around increasing bandwidth and throughput. Currently, this can be achieved using ATM technology. The computer and

telecommunications industry has been actively pursuing ATM technology for more than five years.[8] ATM has the promise of putting gigabits of traffic over one line and, unlike the Fiber Distributed Data Interface (FDDI) technology it will replace, it will be less expensive and will not necessarily need fiber optics technology.

The BNCC needs to take the lead in assessment of their base cabling, network software, and applications to ensure that they will be able to take advantage of ATM and next-generation technology as it becomes available and needed by customers. ATM implementation may require new cabling and network software. While many bases have the internal resources needed to plan and design a network capable of supporting both their data and telephone needs, most lack united goals and the funds to reach them. This lack of a base-wide approach prevents most bases from taking improvement actions under current budgetary constraints.

Recommendation

MAJCOMs and BNCCs should be encouraged to implement existing technologies to address capacity and bandwidth issues. Currently, ATM is an adequate solution; however, BNCCs must be flexible and retain the authority to implement newer technologies as they become "industry standard."

Base-Level Network Management

This section addresses the management challenges faced by the network administration personnel manning the Base Network Control Center (BNCC). BNCCs are faced with the dilemma of increasing responsibilities without commensurate authority. An organizationally isolated control center is held accountable for overall

network management and the challenging issues of Web implementation, network privileges, training, equipment, and funding.

Current Situation

Conceptually, the BNCC *can* have a very significant positive impact on the operational effectiveness of the overall network. Several current Air Force publications support this idea. Air Force Policy Directive (AFPD) 33-1, *Command, Control, Communications, and Computer (C4) Systems,* states the following:

> Effective employment of Air Force resources in a dynamic and demanding world environment requires compact, robust, user friendly, and sometimes highly mobile C4 systems. Those qualities can be achieved only through maximum standardization and adherence to well-conceived and conscientiously enforced architectures. . . .[9]

More specifically, AFI 33-115, *Network Management*, identifies the responsibilities for supporting critical Air Force C4 networks, primarily through BNCCs.

> Network Management (NM) is crucial to providing effective, efficient, and reliable C4 information network services used in critical Department of Defense (DoD) and Air Force wartime, business and C4 processes. The BNCC is the single focal point on each base to provide NM and customer support for these critical services. [10]

The BNCC function, however, was created *after* many unclassified LANs had already been installed. Funds, in most MAJCOMs were not allocated to reroute communications lines or to establish a consolidated network management facility. In fact, AFI 33-115 actually directs the BNCC to use "existing wing resources."[11] However, the instruction also states that "the BNCC is responsible for maintaining network operations."[12] Therefore, the BNCC is in the unsavory position of being responsible for a network that it did not create and cannot modify. In fact, their responsibility is extensive. Specifically the BNCC is accountable for the following services:[13]

1. Help Desk Operation.
2. Network Management.
3. Specific Area of Support (functional experts).
4. Other duties to include configuration management, fault isolation, security management, performance management, accounting management, network planning, and customer support.

The fact that the BNCC has responsibility for base networks without the authority to consolidate the control of these networks makes troubleshooting, upgrading, or monitoring these networks more than challenging. It is a testament to the BNCC personnel, as well as the unit LAN personnel, that most networks have not significantly suffered to date. However, as discussed in the following paragraphs, changes will be needed to upgrade the networks to keep pace with developments like the Web. A central function will be necessary to orchestrate and manage these changes without compromising service or security.

Web implementation has generated several unique challenges for the BNCC. Historically, customers have installed and managed their own Web servers without consulting the BNCC. Consequently, when problems with capacity or configuration arise, the BNCC does not have the information to effect changes. For instance, when their Web server drops out of service, if the customer does not notify the BNCC, the BNCC won't be able to post notice to users that the server is "down." In addition to the usual challenges, inexperienced Web page builders may be putting information on their servers that adds stress to their local network and the AFIN overall. Besides wasting bandwidth transmitting unneeded graphics, poor information structuring may force customers to access several pages of information before they get to what they want. Additionally, outdated information is not always purged in a timely manner allowing

users access to potentially inaccurate data. This issue of standardization of Web home pages is so significant that this project dedicates a section to the subject (see "Web Site Standardization," page 71).

Base network privilege issues also arise from the BNCC dilemma. Web home pages are a good case in point. Some organizations do not have formal procedures in place to control the content of home pages. Often, the originator of the home page is not the network administrator, or even the "webmaster." It is not uncommon for the "owner" of a home page to make changes and not inform the network administrator, or go through any quality control (QC) procedures. Some routine changes can be pre-approved, and it is possible to program the Web server to follow scripts that delete dated pages that have become out-of-date. QC procedures are important to make sure that accurate information is posted as well as information that is approved for release (see also "Copyrights and Releasability," page 30). An example of posting an unapproved home page occurred when a programmer in charge of the Kmart Web site linked the corporate message to an erotic picture. Kmart dismissed the programmer. [14]

Training for network administrators is a common thread through many base network issues. Achieving the appropriate training has been difficult, particularly in highly technical areas such as programming routers, using specific products like HP Openview and Windows NT server applications. Units have had to purchase this training from civilian suppliers, often at premium prices, or do without. On-the-job training standards have varied from command to command. Currently, there is no standardized training criteria for network administrators. An important aspect of training is making the network administrators aware of specific security issues and requirements. There are

significant security risks inherent to the internet and the Web in particular. These issues of training and network security are specifically addressed separately in other sections (see "Administrator Security," page 82, and "Administrator Training," page 89).

Equipment procurement has also been a problem. AFPD 33-1 states "Air Force C4 systems will be consolidated and standardized to maximize resource effectiveness and reduce costs, commensurate with operational requirements."[15] Guidance is one thing, but implementing standard Air Force contracts is another. The positive aspect of contracts such as the Desktop IV contract and its successors is that it contributes greatly to standardization within the Air Force computer systems area. Unfortunately, similar contracts are not available for other elements such as routers, hubs, and connectors. In desperation, organizations such as the intelligence community have started their own "standard" contracts. Although standard contracts greatly enhance the supply community's ability to acquire components, in the past, many units became frustrated with the seemingly long time required to process the contract paperwork. Often, it seemed that the time required to actually obtain requested hardware or software was so long that the requested items were obsolete before they were even delivered.

The final challenge facing a BNCC is funding. Under current policy each unit is responsible for budgeting and administering the funds for its LANs. This makes it difficult for the BNCC to establish a congruent upgrade plan based upon mission requirements. It is an uphill battle in most cases to fight for a Program Objective Memoranda (POM) line item called "Computer Systems Infrastructure." Decision makers often do not grasp the need for special wiring requirements and support equipment like routers, and the implication that these needs have in terms of funding.

Proposed Solution

In order to make progress, the Air Force must shift its thinking of computers from "nice to haves" to "required support." Computer network access, at least at the unclassified AFIN level, must be viewed as essential as telephone, electrical power, and sewer support. That means that a base, if it plans correctly, should have some excess capacity. Network planning experts suggest planning for excess "computer outlets" in buildings. These outlets should be in place even if they are not all initially planned for use or initially planned to be used to capacity.[16] By looking at computer networks as a "utility" function of a base, we can see why there needs be centralized planning for this utility. No one would expect the base civil engineer to manage the base electrical or sewer system if the wires or pipes in a building were owned and managed by the building occupant. Just like users who need more robust electrical power, the communications unit is going to have to plan for a more robust communications network for users that have that requirement today. Additionally, they will have to plan for capacity that may appear "excess" now but *will be* required in the future. Given this outlook, tackling the challenges inherent with the Web and other more recent communications-computer developments looks increasingly possible.

In order to have centralized control of individual base LANs, the BNCC must be recognized as the base authority for network issues. This includes simple things like individual units notifying the BNCC of LAN outages so the BNCC can post a notice to all base users and external internet visitors. Additionally, if the BNCC is to have centralized control, it must have a standard contract with which to buy common network components. This standard contract may be maintained by General Services

Administration (GSA), Air Force, or MAJCOM, and its goal should be to follow industry's lead and acquire state-of-the-art components. At a minimum, these contracts need to address: cabling (both wire and fiber optics), routers, network software, and network management hardware and software. This type of standard contract has been successfully used in the past for other computer hardware and software and should be implemented further.

However, not all customers can be satisfied by the standard contracts. Some units require specialized hardware or software, or a unit may have a timely mission requirement that requires the unit to bypass normal contract paperwork. New standardized contracts must ensure a *flexible* and *streamlined* approach so that the required product is delivered to the unit in a timely manner.

In addition to having standardized contracts for common components, there should be a central base purchasing point for all equipment to include cabling. Certain items such as cabling and connectors should be purchased in bulk via the BNCC. The costs savings could conceivably be enough to justify certain "emergency repair" stocks on most bases.

In order to adequately fund all of these requirements addressed above, BNCCs should have the authority to plan for upgrades ahead of the need via the POM and FY budget system. USAF/SC and USAF/FM should support MAJCOM/SC funding for infrastructure needs, such as cabling and routers, possibly the cheapest and most often neglected part. What has been missing for a long time is top-down direction from the Air Staff on what base SCs should be planning for and how to fund for it. Timelines, or

"drop dead" times, have been missing. In order for a financial manager to defend unfunded submissions, these items are critical.

Additionally, an important issue to all units is their "face to the outside." Centralized policy must exist to formally establish control over who has authority to make changes to network assets. Because base LANs are regularly visited by outside users and civilians, it is very important that all information presented be accurate and approved for release by *appropriate* authority.

Finally, a common thread behind all of these proposed solutions is the concept of training for network administrators. The training should standardized and include specific classes on current technical issues as well as security issues. Training and security are such encompassing issues that they are addressed in their own respective sections (see "Administrator Security," page 82, and "Administrator Training," page 89).

The Air Staff must pull together the policies of the AF/SC, SAF/AQ, and AF/FM to ensure that proper direction and guidance is provided to their MAJCOMs. Further, the Air Staff must direct a review of guidance to MAJCOMs on base networks with the intent of providing each BNCC the manpower, authority, direction, and funding to upgrade their base networks as required to meet mission needs.

Recommendations

The responsibilities and challenges of the BNCC are broad. The following is a list of specific recommendations to enable the BNCC to have the needed authority and capability to address the challenges.

1. BNCCs should be recognized as the base authority for network issues.
2. Flexible and streamlined standardized contracts, maintained by GSA, USAF, or MAJCOM, should be established on appropriate items. The contracts should

closely follow industry trends. These appropriate items *can* include: cabling (both wire and fiber optics), routers, network software, and network management hardware and software. The ability to use waivers, as necessary, should be in place for units whose mission is not enhanced by the standard contracts.

3. BNCCs should be encouraged to stock standard or common network components such as cabling, connectors, and other hardware.
4. BNCCs should have the authority to plan for upgrades ahead of the need via the POM and FY budget system.
5. Centralized policy must exist to establish who has authority to make modifications to network assets.
6. BNCC personnel should have standardized training (see "Administrator Training," page 89 for specific recommendations).

Web Site Standardization

More and more Air Force organizations and bases are using the Web to enhance their mission. Much of the information posted on the Web is not intended to be restricted to military users only, and is available to interested civilians. For example, the DOD maintains the "BosniaLINK" where anyone can visit via a Web browser and learn more about the Bosnia area including maps, pictures, and news releases. Users can send e-mail to US troops stationed there from this home page.[17] This particular site is very popular, it was visited over 250,000 times during the week of 4 March 1996.[18]

People surfing the Web can generate a distinct impression of an organization, a base, and the Air Force in general by the appearance of a Web site. The Air Force is concerned with the impression that other organizations and people both inside and outside of the service, have of it. The Air Force always does its best to present a professional appearance at all times. Uniformed members maintain strict appearance standards, the grass on bases is well trimmed, and the buildings are maintained as well as possible. Appearances are important, and the impression internet users can get from visiting a Web home page can be a lasting one.

Current Situation

Many Air Force organizations have placed home pages out on the Web. However, there appears to be little thought on how to do it or what information to provide. Some of the Web home pages are laid out in a simple, straightforward, and easy-to-use fashion, while others are overburdened by fancy graphics, contain dead-end links, and have a confusing organization. There is no standard. Air Force Web home pages often vary widely between organizations. The Research Survey found lack of structure to be a particular concern for users.

The Defense Technical Information Center (DTIC) has already developed a basic set of standards for Web home page design. The DTIC standards contain many useful tips and pointers on basic user friendly home page construction.[19] Just applying the following basic DTIC standards would significantly enhance the appearance and utility of Air Force home pages.

1. Keep graphics to a minimum. Some Air Force home pages contain so many graphics they can bring a computer to its knees. Graphics are bandwidth intensive and should be used only when necessary or when they provide useful information.
2. Provide a text-only browse capability. Web users should be able to browse through a home page in the text-only mode. "Hiding" links in fancy graphic buttons forces users to download graphics and use up bandwidth unnecessarily.
3. Utilize basic browser navigation functions.
4. Provide a clear path back to the first home page so users can reorient themselves. (for example, double click the "back" arrow or provide a hotlink to the first page on each page.)
5. Ensure that all hotlinks are active.

The Air Intelligence Agency (AIA) has recognized the need for uniform *organizational* home page features and has developed a list of things every AIA home page should provide. While this list is not all inclusive, it provides a good starting point.[20]

1. Organization identification in plain text and acronym form.
2. Security disclaimer.
3. Links to a page with the organization's mission with key two-letter office descriptions and central office phone numbers.
4. Links to the organization's mission, goal, and vision statements.
5. Links key network managers in charge of the Web pages.
6. Links to a page containing a directory of product and services, this page should have a search option, if appropriate.
7. Link to a page containing information on "What's New."
8. Link to a page dedicated to customer support. This page can be used to send messages to the "Webmaster," or the network manager responsible for the home page, access tutorials, server statistics, organization's comment feedback, and other items.
9. Links to other home pages of subordinate organizations.
10. All pages should include a date posted and a point of contact for information on that particular page.

Additionally, *access* to Web pages varies widely between organizations. Organizations can create restrictions to Web sites by only allowing users access with a ".af.mil" domain address or local base address. Basic information, like a unit's mission statement, is sometimes restricted from public access; sometimes it is even restricted from other Air Force users. Organizations within the same MAJCOM and at the same base often provide differing levels of access to the same types of information. Phone and e-mail directories may be openly provided by one organization and arbitrarily restricted by another. The widely varying levels of access present an image of an organization that does not know what it is doing, and the Research Survey results highlighted this lack of consistent access as a significant concern to users.

Current Air Force home pages sometimes contain security banners, or links to pages containing the banners, warning individuals accessing Web sites that they are accessing a government resource and may be monitored. In many cases, the inclusion of a lengthy legalistic dissertation at the top of a local Web page would defeat the legitimate public

relations objectives of an otherwise "friendly" page. Some Air Force home pages greet the public with large-type, boldfaced, and capitalized warning banners that could scare many users away. At the beginning of this study, there appeared to be inconsistent interpretation and application of warning banners on Web sites throughout the Air Force. However, research found that AFI 33-219, *Telecommunications Monitoring and Assessment Program (TMAP),* did indeed address warning banner policy,[21] but may not have been well known across the Air Force. An AIA/DOX interpretation of Section C of the AFI, specific to warning banners (see appendix F), supports the assertion that warning banners were not originally intended to be a universal "rubber stamp" introduction to *all* Web pages. For example, warning banners are not *required* for home pages intended for use by the general public. However, without a warning banner, the legal basis for conducting routine administrative monitoring of computer operations is *greatly* diminished. If a Web page contains restrictive access information, a warning banner *must* be displayed. Web pages that provide access or links to restricted domains should display a warning banner when users attempt to access restricted options. AFI 33-219 recommends the following warning banner:

> OFFICIAL U.S. GOVERNMENT SYSTEM FOR AUTHORIZED USE ONLY. DO NOT DISCUSS, ENTER, TRANSFER, PROCESS, OR TRANSMIT CLASSIFIED/SENSITIVE NATIONAL SECURITY INFORMATION OF GREATER SENSITIVITY THAN THAT FOR WHICH THIS SYSTEM IS AUTHORIZED. USE OF THIS SYSTEM CONSTITUTES CONSENT TO SECURITY TESTING AND MONITORING. UNAUTHORIZED USE COULD RESULT IN CRIMINAL PROSECUTION.[22]

Proposed Solution

Air Force organizations need to clean up their home pages by applying basic common sense standards and adopting a set of uniform features. This will increase the utility of home pages to Air Force members and provide a uniform, professional appearance to the general public.

A survey of existing suggestions from organizations such as DTIC and AIA, coupled with visits to home pages of various Air Force Web sites, leads to the conclusion that there are two categories of home pages. *Base* Web home pages should contain information strictly related to the infrastructure of the base, base personnel listings, telephone directories, and local area information. *Organizational* Web home pages should contain information strictly related to the organization and its mission. Obviously, there should be connections, or links, between the two home pages, but information pertaining to one or the other should be maintained by the respective Web site manager (or webmaster). Information that is not owned by an organization or a base should not be duplicated, but rather, links should be provided to the site that has primary responsibility for the information. Not only should information not be duplicated between the organization and base home pages, each of these home pages may have a requirement for information that is the responsibility of some *other* Web site. For example, the base home pages should provide links to local weather sites. If these sites are available in the local area, perhaps provided by the local city government, then links should point there rather than duplicating the information.

While every organization can and should apply the DTIC standards immediately, there is no list of standard Web page features or set organization for Web pages that units

should employ. Due to the varying missions and unique attributes of different organizations, a standard plain-vanilla Web page will not fit everyone. Also, strict standards can reduce the creativity and hinder the application of new Web features as they become available. However, one example of a standard that could enhance Web home pages is to stress the minimal use of graphics. Currently, bandwidth available to many users is limited and the access time to download graphics can be excessive. Simple text, even text with different font attributes, downloads rapidly. Waiting for extraneous graphics is often tiresome. Even worse are graphics that have links embedded within them. This forces users to wait until the entire graphic is downloaded before performing any operation other than "cancel." In the future, when LAN and internet bandwidths improve for the Air Force user, more and more embedded graphics can be used.

Review of many public-access Air Force *base* home pages has provided good and bad examples of Web home page design. Including many of the good features on Air Force home pages would transform many home pages from simple electronic billboards for public viewing into useful resources for Air Force personnel.

1. Links to base history.
2. Links to local area information, including links to local government home pages, public recreational home pages, and a brief description of local area.
3. Searchable e-mail directory for base personnel.
4. Link to a page containing TDY information. This page should include links to on-line billeting reservations, base maps, maps from the local airport, restaurant listings, hotel listings with telephone numbers, and per diem rates.
5. Link to a page containing Newcomer Information. This page should include base housing information, on-line base housing registration, and local real estate listings.
6. Links to pages containing local weather information. These pages can be maintained by local city services, but should have a brief description of yearly climate, current conditions, and a seven-day forecast.

7. Links to a page containing base facility information. This page should be include commissary and BX hours of operation, recreational facilities hours and fees, hobby shops hours of operation, and other information.

Standardized directory search trees, subject headings, and accessibility rights must accompany the standard web page features to maximize their utility. Currently Air Force Web home pages often contain the similar information, but the categories of information are labeled differently. Users should be able to go from base to base and easily find information. In an effort to create standard Air Force home pages, the best of the reviewed information is presented in figure 4-3, figure 4-4, and figure 4-5. Figure 4-3 is a representation of a standard organization home page with links to figure 4-4, a representation of a standard base home page. Figure 4-5 represents subordinate pages to the base home page.

All of these pages have cross links to each other and links to pages containing supplemental information such as weather conditions or local maps. The important key is that the basis of information, for example the page containing local weather information, should be only in one location, maintained only by one organization. Any page intended to supply this type of information should not maintain the information but should point to the page that actually hosts the root information.

ORGANIZATION HOME PAGE

- Basic Information
  - Simple Organization Graphic or Emblem
  - Link to Mission, Goals, and Vision Statements
  - Link to Organization Commander Biography
  - Link to Key Points of Contact
  - Link to Customer Support
  - Link to Webmaster E-mail
  - As of Date
- Links to Other Information on Organization
- Links to Subordinate and Support Organization Home Pages
- Links to Other Related or Similar Organizations Home Pages
- Link to **BASE HOME PAGE**
- Link to Next Higher Headquarters Home Page
- Link to MAJCOM Home Page
- Link to USAF Home Page

Note: Bolded text refers to another included sample Web page.

Figure 4-3. Sample Organization Web Home Page

BASE HOME PAGE

- Basic Information
  - Simple Base Graphic or Emblem
  - Link to Mission, Goals, and Vision Statements
  - Link to Base Commander Biography
  - Link to Key Points of Contact
  - Link to Customer Support
  - Link to Webmaster E-mail
  - As of Date
- Links to Tenant **ORGANIZATION HOME PAGEs**
- Link to **WHAT'S NEW PAGE**
- Link to **BASE SERVICES PAGE**
- Link to **BASE INFORMATION PAGE**
- Link to **TDY PAGE**
- Link to **NEWCOMERS PAGE**
- Link to **LOCAL AREA INFORMATION PAGE**
- Link to USAF Home Page

Note: Bolded text refers to another included sample Web page.

Figure 4-4. Sample Base Web Home Page

BASE SERVICES PAGE

- Searchable Base Directory
  - E-mail and Phone directories
- Information on Youth Services
- Information on MWR Facilities
  - Hobby Shop hours/rates
  - Class Schedules
- Gym facilities and hours
- Base Education Office Information
- Military Personnel Flight Information
- Commissary/BX services and hours
- Other Information
- Link back to **BASE HOME PAGE**
- As of Date

NEWCOMER'S PAGE

- Housing Office Information
  - Base Housing Registration
  - Real Estate Listings
  - Rental Listings
- Travel Management Office Information
- Variable Housing Allowance Rates
- Link to Base Map
- Link to Local Weather Conditions
- Link to **BASE SERVICES PAGE**
- Link to **BASE INFO PAGE**
- Link to **LOCAL AREA PAGE**
- Link back to **BASE HOME PAGE**
- As of Date

WHAT'S NEW PAGE

- Listing of New Features or Capabilities of Base LANs
- Links to New or Significantly Updated Base Pages
- Link back to **BASE HOME PAGE**
- As of Date

BASE INFORMATION PAGE

- Base History
- Link to Base Map
- Link to Local Weather Conditions
- Link to **BASE SERVICES PAGE**
- Link back to **BASE HOME PAGE**
- As of Date

TDY PAGE

- Link to On-line Billeting Reservations
- Directions from Airport with Map
- Link to Per Diem Rates
- Link to Local Restaurant Listing
- Link to Local Hotel Listing
- Link to Base Map
- Link to Local Weather Conditions
- Link to **BASE INFO PAGE**
- Link to **LOCAL AREA PAGE**
- Link back to **BASE HOME PAGE**
- As of Date

LOCAL AREA INFO PAGE

- Links to Information on Local Area
  - Major Attractions
  - History
  - Maps of Local Area
- Link to Local Chamber of Commerce Home Page
- Links to Other Local Web Pages
- Link to Local Weather Conditions
- Link back to **BASE HOME PAGE**
- As of Date

Note: Bolded text refers to another included sample Web page.

Figure 4-5. Sample Second-Level Base Web Pages

Overly restrictive access to information can defeat the purpose of providing a home page in the first place. Public access home pages should be created as a means of disseminating information to the public and the Air Force community. While access to some information needs to be restricted, the vast majority of restricted access information on Air Force Web pages should be provided to everyone. Some types of information that might be restricted are base roster information such as telephone numbers, e-mail accounts, and other "For Official Use Only" types of information. A list of restricted information should be standardized across the Air Force.

Use of security banners should be standardized as well, across the Air Force. AFI 33-219 is flexible, and *does* allow organizations to modify the warning banner. AIA suggests a "friendlier" security banner for sites available to the general public:

> This is an unclassified US government computer system, provided as a public service. Government personnel and the general public may use this system to review and retrieve publicly available information. The general public may access any publicly available portions of this system. Selected elements of it are subject to access restrictions that are identified in parenthesis next to the data link. You may use any portions that do not restrict your access. Anyone using this government system expressly consents to administrative monitoring at all times. You are further advised that system administrators may provide evidence to possible criminal activity identified during such monitoring to appropriate law enforcement officials. If you do not wish to consent to monitoring, exit this system now.[23]

This study feels that the trend toward friendliness should, in fact, go much further. Perhaps a abbreviated version of the current attempt would truly achieve the desired objective.

AIA also suggests that if the warning banner has already been provided on the initial Web home page, only a simple reminder is required for unauthorized users who attempt

to access restricted domains. A simple message like "*You are not authorized this option*" is sufficient.[24]

Recommendation

1. HQ Air Force shall maintain a set of *suggested* standards of layout and construction that will eliminate the apparent confusion and bring order to Air Force Web pages.
2. Organizations shall not maintain information that they are not directly responsible for. Rather, they will provide a link to the organization that is responsible for the information.
3. Accessibility of information must be uniform across the Air Force. HQ Air Force shall maintain a set of standards concerning information that should be restricted and what information should be provided openly.
4. Ensure network administrators and home page authors understand the intent behind the security warning banner. Home page authors must use a standardized warning banner that is appropriate for the level of access of the information presented.

Administrator Security

As is true with all security risks, computer security risks evolve over time. This is primarily due to computers growing in popularity and computers being used more and more for communications rather than for stand-alone processing. As more computers become networked, groups and individuals with malicious intent have more opportunity to remotely attack computer network systems. An in-depth discussion on the historical growth of computer security risks with specific case studies and examples can be found in appendix C.

Current Situation

One of the first overt actions taken in internet computer security was the forming of the Computer Emergency Response Team (CERT). In 1988, Defense Advanced Research Projects Agency (DARPA) formed the Computer Emergency Response Team

(CERT) in response to needs exhibited during an internet-wide "worm" incident. In November 1988, a worm was released which rapidly brought the internet to its knees when it penetrated over 6,000 internet computers. The CERT Coordination Center (CERT/CC) is located at Carnegie Mellon University's Software Engineering Institute and serves as a focal point for response to internet computer security problems.[25] CERT regularly publishes reports describing computer security incidents.[26]

Another resource that is currently available to LAN administrators is the Security Administator's Tool for Analyzing Networks (SATAN)[27] or similar programs. Even though the introduction of this program scared many users and administrators, its original application was for system administrators to test the security of their own UNIX systems. UNIX systems are common on the internet and some implementations have numerous security holes. Even though SATAN is relatively new, the techniques that it employs are old and outdated by the standards set by the rapidly growing internet (see appendix C).

Recent Air Force action has created the Base Network Control Center (BNCC). The BNCC is the single focal point on each base to provide network management and customer support for these critical computer network related services.[28] Currently, however, the BNCC is the base network control center in name only. The BNCC does not have authority to access or direct routers and networks of organizations on the base. Each organization on a given installation is responsible for maintaining a properly operating and secure internet operation. The result is that the BNCC cannot take immediate corrective action when an attack is underway or when one problem with one organization's computer operations impacts the rest of the base users. When the BNCC

identifies problems it must work through other organizations to resolve the problem. Problems that could potentially be resolved in minutes take hours or days to resolve.

Several formal publications give guidance on security requirements with respect to system administrators. AFI 33-115, *Network Management*, briefly states the need for security considerations but this document was last updated in June 1994, and released on CD ROM in January 1996.[29] It references an even *older* March 1988 security document for more details.[30] AFI 33-112, *Automated Data Processing Equipment (ADPE) Management*, gives security guidance, but this is primarily with respect to the bureaucracy aspects of maintaining a paper trail by base ADPE managers.[31] The recently developed AFMCI 37-102, *Transmission of Information via the Internet*, suggests several actions required by system administrators with respect to security. The instruction declares that "system administration is the key to preventing intrusion."[32] Additionally, administrators should audit incoming and outgoing user activity to identify possible security threats, and they should maintain a close working relationship with the Information Protection Office of the Air Force Information Warfare Center.[33]

These are just a sampling of some of the publications that mention the responsibilities of the administrator with respect to security; however, as can be seen, none go into great detail. Finally, AFMCI 37-102 succinctly states perhaps the best enhancement to security when it emphasizes the need for adequately trained system administrators:

> The skill and knowledge level of the systems administrator, in concert with the applied technical solutions or "patches" available, usually is the key determinant in keeping a system and its information secure. [34]

Many administrators are using a common hardware device called a "firewall" to improve security of their system. A firewall is a dedicated computer or router with special software that is situated between the internet and the LAN. The firewall is used to implement policy and enforce service and user access restrictions. The firewall blocks and monitors transmissions going back and forth between the internet and the LAN.[35]

Many of the required elements for improving the security of Air Force internet operations are already available or are under development. The Air Force Network Strategy Office (AFNSO), an office within Air Force Command, Control, Communications, and Computers Agency (AFC4A), is developing a firewall solution called Info Protect Barrier Reef.[36] This project was initiated to provide a secure solution for those customers who need to connect to the base network and to an outside network not meeting the security criteria of NIPRNET. For example, Air University is currently developing a plan to have both direct connections via the education domain (.edu) and the military domain (.mil). In this case, Air University will need Barrier Reef-type protection to isolate the base network from the worldwide education domain. Another example of using Barrier Reef would be a base hospital that wants to tie into a local network to connect with on-line civilian medical databases. The hospital will also want to connect to the base network which in turn is connected to the rest of the military domain. Barrier Reef is essentially a two-router scheme. One router, identified as the external router, provides protection between the base computers and the internet. The external router provides general packet filtering of incoming traffic and very little filtering of outgoing traffic. The internal router performs the bulk of the security operations, such as filtering packets, limiting services, and determining degrees of access from the internet.

An important element of the Info Protect Barrier Reef project is to depend on the BNCC to consolidate base internet operations. Centralized internet operations will alleviate other base organizations of the responsibility of maintaining separate internet routers. Consolidating internet operations will also eliminate the duplication of effort between organizations trying to run a secure internet operation (see "Base-level Network Management," page 63).

Proposed Policy

From the above discussion three main issues surface with respect to the administrator network security. Centralized Air Force internet policy is lacking. There are various hardware and software security solutions available. Training and security awareness is lacking.

Air Force organizations have been hooking up computers to the internet without a clearly defined security policy. While the Air Force and DOD are developing technical security solutions to internet security problems, there is currently no *centralized* Air Force level internet security policy. The problem stems from the fact that a computer hooked up to the internet becomes both a computer *and* a communication device. The majority of computer publications like the DOD "Orange Book"[37] are intended for stand-alone computers and do not adequately address internet security problems. Portions of policies intended for communication equipment, such as telephones (see "Official Use," page 35) can be applied to internet computers, but the result is less than satisfactory. What is needed is a fusion of currently applicable policies and the development of internet-specific policies into a comprehensive Air Force internet security policy. The BNCC is a

step in the right direction in consolidating official internet responsibilities, but the BNCC must have sufficient base-wide authority to react to security threats.

Hardware is another valuable tool to the LAN administrator in preventing security intrusions in computer networks. Many advances have been made recently in firewall and router technology. Firewalls ease the system administrators task by placing all security operations into single computer; however, firewalls are not a panacea. Currently, there are limitations to these hardware solutions. One limitation may be that as firewalls restrict access, they also restrict throughput, potentially slowing down the entire network. Additionally, even though they may restrict access, current firewall technology is not advanced enough to screen out viruses before allowing infected files on the network. Another limitation is that the firewall or router becomes a single-point failure. If the firewall fails or if a security hole is discovered, the rest of LAN could potentially be laid open to the intruder. Because of these, and other limitations, firewalls and routers must be monitored constantly.

The Info Barrier Reef example cited above is just one example of technology providing superior security protection. However, similar to combat electronic warfare, where each electronic measure (radar) forces an electronic countermeasure (ECM or jamming) which in turn forces a electronic counter-countermeasure (ECCM), internet security countermeasures spawn internet security counter-countermeasures. In other words, the threat evolves with the technology. Therefore, protection technology cannot stagnate.

Although users are ultimately responsible for the security of their own computer, system administrators have a responsibility to inform the user of what needs to be done.

Some users may be reluctant to regularly change their password. System administrators should configure the LAN to require users to periodically update their password. The LAN server could be configured to provide the user with a generated random alphanumeric password. These type of random passwords are much harder to "hack," unfortunately, these random passwords are difficult for users to remember and often create more problems than they are worth. A better solution is to employ advanced authentication techniques in the form of smart cards, tokens, and one-time password software programs. Advanced authentication techniques make it easy for the user and significantly enhance security.

A previous section discussed the need for a trained LAN administration staff (see "Administrator Training," page 89). The previous argument centered primarily on making the staff more efficient. However, LAN administrators must have specific training on security, as well. Without training, LAN administrators may not know to regularly check the CERT listings for new reports that may improve the security of the systems that they are responsible. UNIX systems in particular are known for their security vulnerability. It is incumbent upon the system administrator to be aware of all of these security holes and plug them. Even though most of these security problems are well known, many system administrators have not taken care of them, resulting in hacker attacks and compromised data.[38] In addition to pure security training, network administrators must be aware of the requirements levied upon them to maintain security accreditation packages, as well as how to accomplish those requirements.

Putting together a secure internet connection starts with a comprehensive internet administration policy. Numerous publications, instructions, directives, policies, and

guidelines exist to guide the Air Force user. However, the more restrictions that are placed on these services, the less the Air Force will benefit from the internet. Additionally, many of these publications do not address the current state of technology. Finally, the vast number of publications distributed by individual organizations, the Air Force, and the DOD make understanding the *overall* internet policy difficult, and thus compliance unlikely.

One could suggest that the only secure computer is one that is turned off and never used. Fortunately, there is an alternative to turning off and locking up all the computers. Secure internet computer operations consist of several things: a comprehensive internet administration policy, hardware solutions such as firewalls, software solutions such as advanced authentication techniques, and properly trained personnel.

Recommendation

Establish a separate centralized publication, subordinate to the capstone policy, addressing security issues on the Air Force Internet (AFIN). Review BNCC responsibility and authority to ensure that it can adequately respond for the base in the event of a base-wide security threat. Implement an Air Force-wide training program for LAN administrators (as described in "Administrator Training," page 89). This training should focus on security issues such as hardware and software protection schemes.

Administrator Training

Current Situation

None of the reviewed policies and guidance specified *mandatory* training requirements for computer administrators. AFI 33-115, *Network Management*, references

"positional certification" several times with the implication that network administrators should be certified; however, it does not specify the mechanism for this certification. It also provides guidance concerning training, but again, it provides no specific mandatory direction for organizations to follow.[39] Some organizations require training for new users.

Many organizations require their computer administrators to have a "communications" background. The organizations usually desire that the personnel have technical knowledge and an interest in computers. This, however, is usually as far as the requirements go. Just because a person has a background in computers or in communications does not give him the necessary knowledge to be a computer LAN administrator.

Several examples that were uncovered during analysis of comments from the Research Survey can highlight this shortcoming. One example related a story involving a LAN administrator who helped an individual that had accidentally corrupted his computer's boot-up configuration files. The administrator manually recreated a long and involved sequence of commands from memory and typed them into the user's computer. The administrator then tried booting up the computer to see if the files were correct. Although the administrator was "computer motivated" and certainly "computer smart," he had received no formal training in network administration and apparently did not know the technique of using a bootable floppy disk that contained all of the *standard* boot-up files.

Another example of lack of training occurred at an organization when a user sent an e-mail to the administrators. The administrators misunderstood the contents of the e-mail

and assumed that the user had compromised his password. The administrators changed the user's password and then notified him of his changed password *via e-mail.* Of course, the user could not logon to get the e-mail that notified him of the changed password. With training, the LAN administrators might have taken a different approach. They would still err on the side of security and change the user's password; however, they would have found a different way to notify the user. Other ways include: sending e-mail to someone who works close to the user, making a "broadcast" e-mail explaining to users why their office mate cannot login, or even an "old-fashioned" walk down the hallway to tell the user in person or to leave a "yellow sticky note."

Proposed Policy

All computer LAN administrators should receive mandatory training in network administration and security. Offices cannot depend on the "interested and knowledgeable" person to be the best-qualified administrator. As technology increases, it becomes very hard for someone to know the latest techniques or understand the latest hardware or software without specific training, and it should be the commander's responsibility to ensure personnel practice correct procedures.

Network administrators *should* be communications people. But, in any case, after specific LAN administration training and after working at the job for a minimum amount of time, the person's duty record should reflect his network administration expertise. It is not a new idea to require Air Force personnel to have a documented proficiency in a career field. Enlisted personnel are normally required to demonstrate proficiency in the tasks designated in their training records, pass the required Career Development Course material, and serve a designated time in that job to upgrade to a higher skill level.

Officers in the acquisition career field must possess a certain level within the Acquisition Professional Development Program (APDP) to be considered for many responsible jobs in acquisition. There are three levels within APDP and each level has formal training, experience, and academic education requirements. There are many acquisition courses sponsored by the Air Force Institute of Technology (AFIT) and the Defense Systems and Management College (DSMC) that provide this formal acquisition training. AFIT and DSMC are not manned sufficiently to provide all of the training for the acquisition corps. Therefore, AFIT often contracts to civilian companies to come to bases to provide standardized training courses. Similarly, Air Education and Training Command (AETC) could contract training courses to civilian suppliers. It is often easier for specialized civilian companies to keep abreast of rapidly-changing technology, such as firewalls, routers, and network software. Security issues, in particular, are of obvious importance to the network administrator and therefore should be stressed in formal training (see "Administrator Training," page 89).

There are several courses in existence today that would more than adequately train new and existing administrators on proper LAN administration and security. One such course is "Network Security Vulnerability Technicians Course" for LAN administrators.[40] Many other courses exist. The federal government maintains a Web home page dedicated to advertising computer-related training courses. This Web site lists over 15,000 training courses.[41]

It is not just the administrators that need training. There is no requirement for supervisors and commanders throughout the command chain to have formal internet training. In other words, the policymakers, both those making overall Air Force

decisions, and those signing new publications and guidelines, may not be aware of how this rapidly-changing technology affects their particular mission. A mechanism should be put into place to educate these decision makers about the internet and its potential for exploitation.

Recommendation

Mandate that LAN administrators take formal training in network administration, and a system be developed to track and document personnel proficiency. Develop and implement a training program for senior Air Force leadership to educate them on the implications of the internet.

Notes

[1]Mr. Charles Hall, Systems Engineer, Silicon Graphics Corporation. Briefing to ACSC Students, 13 December 1995.

[2]Darrel Beach, DDN Program Management Office, interview with Maj Matonak, 14 February 1996.

[3]"CNN Interactive." [On-line]. Available HTTP: http://www.cnn.com [1996, February 9].

[4]Beach.

[5]AFI 33-115 *Network Management*, 24 June 1994.

[6]Position Paper on the Information Project Barrier Reef, AFC4A, 5 January 1996.

[7]Beach.

[8]AFDIR 33-121, Compendium of C4 Terminology, Atch 1, 5 July 1995.

[9]AFPD 33-1, *Command, Control, Communications, and Computer (C4) Systems*, para 1.1.

[10]AFI 33-115, para 1.

[11]Ibid, para 2.

[12]Ibid, para 3.1.2.

[13]Ibid, para 3.3.

[14]Marc Gunther, "Goofing off at the office goes high-tech." *Montgomery Advertiser*, 24 March 1996, 5F.

[15]AFPD 33-1.

[16]Mr Ken Kanagaki, MITRE (AIA/SCM), Kelly AFB TX, interview with Maj Matonak, February 95.

[17]"BosniaLINK," Office of Assistant Secretary of Defense Public Affairs [On-line]. Available HTTP: http://www.dtic.dla.mil/bosnia/ [1996, March 11].

Notes

[18]Col Michael Perini, HQ ACC/PA, briefing to ACSC students and faculty on 11 March 1996, Military-Media Relations Symposium.

[19]"DTIC WWW Server Standards and Guidelines." (24 April 1995). Defense Technical Intelligence Center (DTIC) [On-line]. Available HTTP: http://www.dtic.dla.mil/staff/ trefzger/standards.html [1996, March].

[20]*Intelink Concept of Operations for AF-wide Implementation* (draft), AIA/SCXP, 25 July 1995.

[21]AFI 33-219, *Telecommunications Monitoring and Assessment Program (TMAP)*, 12 June 1995.

[22]AFI 33-219, para 16.3.5.

[23]Col Livingston, AIA/DOX, to Lt Col Kelso, AU/RCO, letter, subject: Clarification to AFI 33-219 (Your Memo, 13 December 1995), 2 February 1996.

[24]AIA/DOX letter to Lt Col Kelso.

[25]Richard D. Pethia and Kenneth R. van Wyk, *Computer Emergency Response - An International Problem*, Pittsburg, PA: Computer Emergency Response Team/Coordination Center, Software Engineering Institute Carnegie Mellon University, Pittsburgh, PA, (14 November 1990). [On-line]. Available HTTP: http://www.riken.jo.jp/ archives/security/cert/info/security.response.cert.txt [1996, February 28].

[26]CERT Coordination Center FTP Server, public directory. Pittsburg, PA: Computer Emergency Response Team/Coordination Center, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA., (no date). [On-line]. Available FTP: ftp://cert.org/pub [1996, March 15].

[27]Wietse Venema and Dan Farmer (24 April 1995). *Security Administrator's Tool for Analyzing Networks* [On-line]. Available HTTP: http://www.fish.com/satan/ [1996, March 16].

[28]AFI 33-115.

[29]Ibid.

[30]DOD 5200.28, *Security Requirements for Automated Information Systems (AIS)*, 21 March 1988.

[31]AFI 33-112, *Automated Data Processing Equipment (ADPE) Management*, 6 May 1994.

[32]AFMCI 37-102, *Transmission of Information via the Internet.* (1996) [On-line], paragraph 7.1.2.3.4. Available HTTP: http://www.afmc.wpafb.mil:12000/publications/ AFMC_Instructions/37-102.doc [1996, February 21].

[33]Ibid, paragraph 6.2 and 7.1.2.3.

[34]Ibid, paragraph 7.1.2.3.

[35]National Institute of Standards and Technology, NIST Special Pub 800-10, [On-line]. Available HTTP: http://csrc.ncsl.nist.gov/nistpubs/800-10/ [1996, January 17].

[36]Position Paper on the Information Project Barrier Reef.

[37]DOD 5200.28-STD, *Department of Defense Trusted Computer Evaluation Criteria* ("Orange Book"), 26 December 1985.

[38]Stoll, Clifford, *The Cuckoo's Egg*, New York, NY: Doubleday, 1989.

[39]AFI 33-115, para 6.6.8 and 7.

Notes

[40]Capt Schu, USN. Briefing to ACSC students/faculty. "Information Warfare." 29 November 1995.

[41]*Fed Center* (1995). The Interfed Group. [On-line]. Available HTTP: http://www.fedcenter.com [1996, March 26].

Chapter 5

Conclusions

Five broad challenges emerged from the analysis of this project. (1) There is a lack of robust and durable, centralized internet policy. (2) There are no common standards for Air Force use of the internet. (3) Networks, both long-haul and base-level, face perpetual capacity and bandwidth problems. (4) Roles and responsibilities of Air Force personnel using and managing the internet are poorly defined. (5) Current training for both individual users and network managers is inadequate and is not keeping pace with the rapid advance of technology.

This study embarked with the objective of assessing the state of, what is essentially a technological revolution that deeply affects the United States Air Force. Very quickly, research showed that the revolution, that is the internet, has not been paced by Air Force policy. Indeed, as this study viewed the entire Air Force policy framework, using the pyramid model (figure 1-3), a conglomeration of several disparate and widely-dispersed subordinate command publications emerged. AFMCI 37-102, *Transmission of Information via the Internet,* is a good start, but with the rapid growth of the internet as a critical tool for mission support, MAJCOM-level guidance is insufficient and begs for the creation of a headquarters-level capstone internet policy.

A *capstone* Air Force internet policy would have the goal of contributing to efficiency and effectiveness by directing time-tested methods, restricting known inefficient behavior, and standardizing equipment, training, and responsibility as it concerns internet operations. This policy should address both the user and network manager separately by providing direction and information tailored to each unique environment. Additionally, due to the accelerating pace of technological advances, this policy must be written so as to be durable enough to stand the test of time, measured often in days, not years. With these precepts in mind, the majority of this study explored the specific content required to ensure a truly worthwhile Air Force internet policy.

The combination of literature search, survey, interview, and debate generated a definite pattern of issues that are currently considered important to the application of the internet in the Air Force environment. Some issues had applicability to both the user and network manager communities, while the majority were ultimately specific to one or the other.

Applicable to both communities, were concerns over capacity and training. The capacity problem may be likened to keeping freeway modernization ahead of population growth. The Air Force already suffers many traffic jams. Both communities can take steps to minimize that problem. Of all the issues addressed, though, this study found that emphasis on judicious training of both the user and network manager could have the most far-reaching effect on Air Force internet productivity.

The Air Force internet user is caught in the middle of a rapidly-expanding technology that is, for the most part, devoid of reference or doctrine in Air Force circles. This study found, however, that the internet environment is as much an evolution as it is a

revolution. By simply applying commonly-understood standards of professionalism and courtesy, time-tested in telephonic and written media, the internet user has already solved many of the concerns, that for some reason, have dogged advocates of this promising technology. Perhaps the most legitimate underlying concerns are the very real security hazards presented by this media. Whereas *classified* Air Force data flow was long ago segregated from the internet realm, the bulk of variably-sensitive *unclassified* Air Force transmissions are scantily protected, if at all. Off-the-shelf encryption technologies exist to mitigate this hazard. In any case, user security awareness will have an immediate effect with little or no "money down."

To an even greater extent than the user, the Air Force internet network manager must deal with a technology explosion that has advanced significantly beyond the physical and organizational capabilities of most bases. This study found that network managers should energetically advocate funding for more simplified and higher-capacity networks to meet the increased demand dictated by software-intensive applications such as the Web. To assist the network manager, unifying concepts, such as the BNCC, should be employed and fully supported in order to reduce duplication and centralize control. At stake is not only user convenience, but in fact, the very *image* of the United States Air Force as a professional, global organization. Every day, presentations as simple as a base-level home page, portray an unmistakable image to an uncountable audience on a worldwide stage. Otherwise dry topics, such as Web page standardization, take on a totally new significance in this context.

With the coming of age of the internet phenomenon, the Air Force finds itself struggling with all the expected awkwardness associated with any leading-edge

technology. Not unlike the current trend towards military jointness, the internet demands carefully-crafted training, the establishment of *common* standards, and most importantly, the formulation of sound doctrine. It is to those ends that this study engaged the challenges of the internet and contributed guidance that could ultimately benefit that fledgling virtual community known as the Air Force internet.

Appendix A

Capstone Internet Policy

The following document is a notional Air Force Policy Directive based on the results of this study. This document is not comprehensive, its primary purpose is to realistically portray a baseline of policy issues that this study found to be central to internet employment.

BY ORDER OF THE SECRETARY OF THE AIR FORCE

AIR FORCE POLICY DIRECTIVE XX-XXX
1 April 1996

INTERNET POLICY

The policy provides capstone guidance for the use and administration of the internet in support of the Air Force mission. It is not intended to be all encompassing, but rather, proposes key tenets of effective internet employment coupled with a philosophical framework.

1 USER GUIDELINES

1.1 **Individual Communications.** For the purposes of this policy, the term "e-mail" shall include any text, audio, or video message transmitted asynchronously via digital networks.

1.1.1 **Prohibited e-mail:**

1.1.1.1 Commercial e-mails. Any "for profit" solicitation from other than approved USAF activities.

1.1.1.2 Personal solicitation. Any personal ads "for profit." Individual merchandise for sale should be put on a central electronic BBS instead.

1.1.1.3 Chain e-mails. Any unofficial e-mail designed intentionally to solicit multiple forwarding.

1.1.2 **Restricted e-mail:**

1.1.2.1 Cultural and religious messages. Origin shall be specifically limited by unit-level guidelines.

1.1.2.2 Humor. Transmission shall be limited to immediate work area for multiple forwards.

1.1.2.3 Charitable solicitations. Origin and volume specifically limited by unit-level guidelines.

1.1.3 **E-mail techniques:**

1.1.3.1 Shotgun messages. Minimize all multiple forwards and multiple replies. Strive to address messages to a *minimum* target audience. Legitimate workgroup list

addresses *are* encouraged. Use electronic BBSs whenever possible.

1.1.3.2 Staffing. E-mails representing an organization must be staffed, if applicable.

1.1.3.3 Quality message. Refer to Air Force Handbook 37-137, *Tongue and Quill,* to ensure editing for impact.

1.1.3.4 Inbox management. Check inbox daily and delete unwanted messages.

1.1.3.5 Storage. Download or extract mail messages to files then to disk for future reference.

1.1.3.6 Sensitivity. Avoid sending or storing "sensitive" text. All e-mails *are* subject to monitoring.

1.1.3.7 Brevity. Keep messages short and to the point.

1.1.3.8 Focus. Center on one subject per message and include a pertinent subject title, so the recipient can locate the message quickly.

1.1.3.9 Emphasis. Capitalize words (SHOUT) only to highlight an important point or to distinguish a title or heading. *Asterisks* surrounding a word also can be used to make a stronger point.

1.1.3.10 Chain of Command. Follow the command chain for corresponding with superiors.

1.1.3.11 Tone. Maintain a professional tone. E-mail is easily forwarded.

1.1.3.12 Forwarding. Avoid forwarding a personal mail without the original author's permission.

1.1.3.13 Signature. Include at least name, rank, organization, and e-mail address, at the bottom of e-mail messages. Optional information could include your organization address and DSN number.

1.1.3.14 Precedence. Assign a precedence (for example, Routine, Immediate, . . .) to e-mails whenever possible.

1.2 **Privacy:**

1.2.1 Several of the prohibitions, restrictions, and techniques pertaining to privacy, particularly confidentiality and solicitation, are interlaced within the guidance on Individual Communications.

1.2.2 Organizations should promote awareness of "safe computing" habits that will preclude the majority of privacy intrusions that commonly occur. Specifically, all personnel should be made aware of the potential for unanticipated message forwarding, in order to take steps to guard against unwanted exposure.

1.3 **Cultural Issues:**

1.3.1 Cultural sensitivity is not unique to the internet. Refer to Air Force Pamphlet 36-2705, *Discrimination and Sexual Harassment,* which details techniques for recognizing and solving discriminatory problems, to include techniques of effective communication.

1.3.2 Organizations should emphasize to personnel that there is an increased danger of *inadvertent* discrimination or harassment in the "cyber-medium."

1.4 **Copyright and Releasability:**

1.4.1 Incorporate lessons in user training that copyright protection rules protect intellectual property creators and the Air Force alike.

1.4.2 Review public affairs and security requirements for information to be released on the Web.

1.4.3 Set up organizational accounts to ensure each unit speaks with "one voice."

1.5 **Official Use.** Use of the internet is limited to what is in the best overall interest of the federal government. Use of the internet is very similar to use of the government telephone system. This includes use of government resources for official use, use that is additionally authorized, and a reasonable amount of personal use.

1.5.1 Official Use. Normal work related internet use and a reasonable amount of internet use to increase professional knowledge on how best to exploit the medium.

1.5.2 Authorized Use. Includes a reasonable amount of personal use to include such things as: emergency communications; communication to family members while the member is traveling on official business; and normal personal communications such as a prudent amount of e-mail, real estate downloads, and communications with an auto or home repair service.

1.5.3 Reasonable Amount. Amount of personal internet use is similar amount of personal telephone use. Local commanders will retain jurisdiction on defining limits of reasonable use.

1.5.4 Disallowed Sites. Local network administrators or commanders shall not generate lists of "disallowed" sites, but rather train individual users which type of sites not to access.

1.6 **Data Download:**

1.6.1 There are four main categories of inappropriate downloads: offensive or obscene material, excessively large files that take up large amounts of system bandwidth, non-official business, and non-certified software.

1.6.2 Computers that are capable of downloading files must have automatic virus-checking software installed. This software must be updated frequently and automatically by the LAN administrator.

1.6.3 Software-testing facilities must quickly address new features on the Web and the remainder of the internet to provide input to policy makers.

1.7 **User Security:**

1.7.1 Sensitive Unclassified Information. Organizations should consider implementing protection techniques such as simple and available encrypting for unclassified, yet sensitive, e-mails and data transfers. Centralized guidance should be provided to individual organizations on suggestions for training courses for users.

1.7.2 Unit commanders have the responsibility of ensuring compliance with proper computer security practices.

1.8 **User Training:**

1.8.1 Individual organizations should provide flexible internet training to personnel dependent upon the degree of user proficiency and mission requirements.

1.8.2 Organizations should encourage personnel to take advantage of training to familiarize themselves with common applications, user etiquette, and security awareness. This allows users to better exploit new technology to enhance the mission.

2 ADMINISTRATOR GUIDELINES

2.1 **Long-Haul Networks Capacity.** For Air Force Web users to see adequate response times, good connectivity to the rest of the DOD community is essential. Future programs should support the reduction of choke points as well as increased bandwidth between core Air Force bases.

2.2 **Base-Level Capacity:**

2.2.1 MAJCOMs and Base Network Control Centers (BNCCs) are encouraged to implement existing technologies to address capacity and bandwidth issues.

2.2.2 BNCCs must be flexible and retain the authority to implement newer technologies as they become "industry standard."

2.3 **Base-Level Network Management:**

2.3.1 BNCCs are the base authority for network issues.

2.3.2 BNCCs are encouraged to submit inputs for flexible and streamlined standardized contracts on appropriate items. These contracts shall be maintained by MAJCOMs and should closely follow industry trends. These appropriate items *can* include: cabling (both wire and fiber optics), routers, network software, and network management hardware and software. The ability to use waivers, as necessary, must be in place for units whose mission is not enhanced by the standard contracts.

2.3.3 BNCCs are encouraged to stock standard or common network components such as cabling, connectors, and other hardware.

2.3.4 BNCCs have the authority to plan for upgrades ahead of the need via the budget system.

2.3.5 MAJCOMs will establish OPRs for base-level network modifications.

2.3.6 BNCC personnel should have standardized training.

2.4 **Web Site Standardization:**

2.4.1 HQ Air Force shall maintain a set of *suggested* standards on Web page layout and construction that will eliminate existing confusion and bring order to Air Force Web pages.

2.4.2 Organizations shall not maintain information that they are not directly responsible for. Rather, they will provide a link to the organization that is responsible for the information.

2.4.3 Accessibility of information on Web pages must be uniform across the Air Force. HQ Air Force shall maintain a set of standards concerning information that should be restricted and what information should be provided openly.

2.4.4 Ensure network administrators and home page authors understand the intent behind the security warning banner. Home page authors must use a standardized warning banner that is appropriate for the level of access of the information presented.

2.5 **Administrator Security:**

2.5.1 Establish a subordinate centralized publication addressing security issues on the Air Force Internet (AFIN).

2.5.2 BNCC has the responsibility and authority to respond for the base in the event of a base-wide security threat.

2.5.3 Standardized training programs for local area network (LAN) administrators will focus on security issues such as hardware and software protection schemes.

2.6 **Administrator Training:**

2.6.1 LAN administrators shall take formal training in network administration and their proficiency will be tracked.

2.6.2 Senior Air Force leadership will receive training on the implications of the internet.

Appendix B

Portrait of the Internet

Internet Defined

Determining a definition of the internet is often contentious. Some authors differentiate between the "Internet" (capitol "I") and "internet" (small "i") where the "Internet" is just one of many global and connected networks and the "internet" refers to all networks connected to one another.[1] One internet authority, John Quarterman, maintains that the overall global network of computers should be called the "Matrix."[2] Quarterman insists that only networks on the "Matrix" that are capable of interactive services (for example, World Wide Web (WWW or Web), gopher, telnet, and FTP) should be considered "on the internet." This definition leaves out significant global networks (for example, UUCP, FidoNet) that are only capable of asynchronous communication (non-interactive). Quarterman also develops a distinction between "supplier-capable" computers and "consumer-capable" computers or networks. "Consumer-capable" computers exist behind a "firewall" and only allow interactive services one-way communication out and, therefore, attempt to protect their internal networks from outside viewing. "Supplier-capable" networks do not have firewall protection and allow outside users to enter their systems for two-way interactive

communications. Many DOD networks are set up with a firewall between the network and the rest of the internet. A firewall is "a form of access-control technology that prevents unauthorized access to information resources by placing a barrier between an organization's network and an unsecured network."[3] Quarterman also insists that the internet consists only of networks that use IP (Internet Protocol).

The Air Force Internet Network (AFIN) is the primary connectivity for Air Force users at the unclassified level. AFIN connects to the government Nonclassified IP Router Network (NIPRNET) at two bases (near Montgomery, Alabama and San Antonio, Texas) via an ethernet connection, creating potential bottlenecks between AFIN and NIPRNET. NIPRNET, in turn, connects with the rest of the internet at only two locations (near San Diego, California and Washington D.C.), further creating potential bottlenecks.[4]

The above samples of definitions of the internet are too restrictive. By trying to too tightly define the internet, the above authors dilute the main point of the internet, a global interconnection of computers and, therefore, users. This study uses the following for a working definition of the internet:

> The internet is a global connection of computer networks and computers. Any computer that can communicate or share information or files with other computers on the common global network is considered "on the internet" or rather, "has access to the internet."

This definition corresponds with AFDIR 33-121, *Compendium of C4 Terminology*, that defines the internet as "a worldwide interconnection of individual networks operated by government, industry, academia, and private parties." [5]

This communication, or interconnection, can be interactive (Web, gopher, telnet, FTP) or asynchronous (e-mail and USENET). Some networks and computers may have

limited internet services, some may have a vast array of services, some may be "protected" behind a firewall (like most DOD networks, or commercial on-line services such as CompuServe or America Online), and some may be open to the world. Some networks are self-contained (for example, isolated classified LANs) and, therefore, are not considered on the internet. *The key is that the computer can communicate in some form with another computer on a global basis.*

Internet Services

There are many services (or tools) available on the internet. Not all services are available from all networks and some networks can only support asynchronous (non-interactive) services. Below is a list of some of the more common internet services:

Electronic Mail (e-mail). E-mail is a system for exchanging electronic messages between users or between computers on the internet. E-mail can include personal messages, official records, and even automatic communications from computer to computer.

USENET Newsgroups. Newsgroups are discussion groups where people focus on a specific subject, such as *rec.arts.startrek.current.*

ListServ mailing lists. Mailing lists are e-mail-based discussion groups. Instead of being sent to a specific individual on the list, messages are sent to a ListServ address so it can be distributed to everyone who subscribes to the list.

File Transfer Protocol (FTP). FTP is a tool for transferring files between computers on the internet. FTP can be used to retrieve and send files from and to a remote host computer. Computers configured for FTP often allow "anonymous" login, or rather, the user attempting to access the host computer does not have to have an account

on the host computer. Often, the host computers are configured to allow "read-only" or allow the anonymous user to download files only.

Telnet. Telnet is a tool to allow logons to remote host computers. Typically, this is to access public files and databases, and even run applications on the remote host. Telnet host computers can be configured to allow "anonymous" logon to anyone or restricted logon to only users with authorized accounts on the host computer.

Gopher. Gopher is a tool to browse certain internet resources. Gopher clients and servers are configured to provide a menu system for "navigating" the internet.

Archie. Archie is a service that indexes thousands of FTP sites based upon a user-provided filename.

Veronica. Veronica is a tool to help find gopher server(s) containing desired information. Veronica menus can be browsed similarly to a gopher menu.

Wide Area Information Server (WAIS). WAIS is a system to search internet databases. Keyword searches can be performed using WAIS to retrieve all of the matching documents.

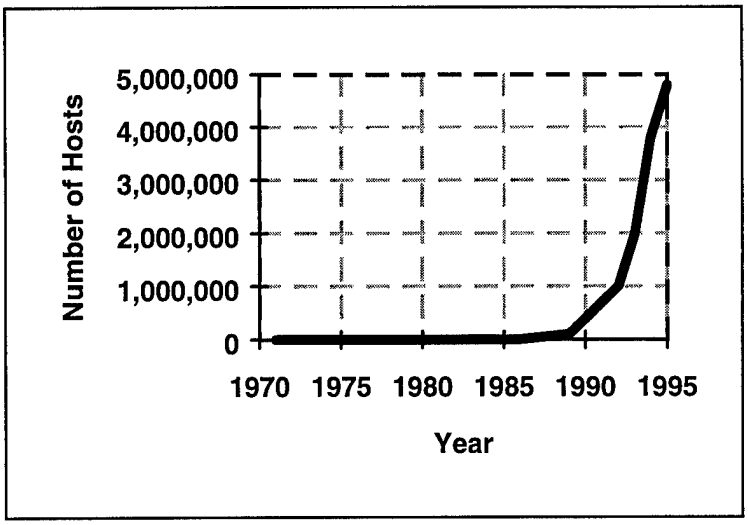
World Wide Web (WWW or Web). The Web is an internet service that enables the internet to browsed by using hypertext links. The Web uses hypertext transfer protocol (HTTP). When a hypertext link is selected, the browser software connects to the specified server (the server could be the local host or could be a remote server) and downloads the information specified by the link at that server site. Once the information is downloaded, the server disconnects until the next hypertext link is selected. The information can be text, graphics, or other multimedia information such as sound or video. Most Web browser software allow the user to access Web sites as well as FTP and

gopher sites. The Web is the first technology to allow users with different processors and different operating systems to exchange information freely without the use of expensive "client" software required for client-server applications.

Internet and Web Growth

Determining the size of the internet and of the Web in particular is a nebulous task. There are several ways in which organizations and individuals attempt to measure the size and growth of the internet. One way would be to track the "domain." A domain is similar to a postal address. On the internet, addresses are specified as Uniform Resource Locators (URLs) which can include specific file information as well as the domain information. The highest level is the last part of the address, such as the ".mil" of a military address.

For example, an address at Air University may end with ".au.af.mil." This address indicates a military address, associated with the Air Force, at Air University. However, domain growth figures only tell you about large organizations, not networks, hosts, or users. Another measure is the number of hosts, or computers, actually serving information on the internet (figure B-1).



Source: Kristin Jacobsen, "Time To Put the Internet in Perspective," *C&RL News*, Mar 1995, p144-147.

Figure B-1. Number of Internet Hosts

Counting the number of hosts is done by sending a message out and counting the number of unique responses (this is referred to as "pinging"). However, many hosts may or may not respond to the ping because they may be behind a "firewall" or may even be off-line at the moment of the ping. Another way to measure the relative growth of the internet is to monitor and measure the number of "packets" or packages of information and bytes of information being transferred by one of the major network "backbones" (such as the NSFNET).

Measuring the number of actual users on the internet is even more daunting. Because of the incredible commercial market potential of the internet, there has been a great deal of study into determining the numbers and demographics of internet, particularly Web, users. Commercial on-line services can, of course, measure their clients reasonably accurately. However, the experts have generally agreed that it is not possible to accurately measure the total numbers of internet users at this time. Some of the difficulty comes from users connecting from behind firewalls or commercial services.

These users do not have unique IP address, and therefore, a particular user can not be consistently identified from one connection to the next.[6]

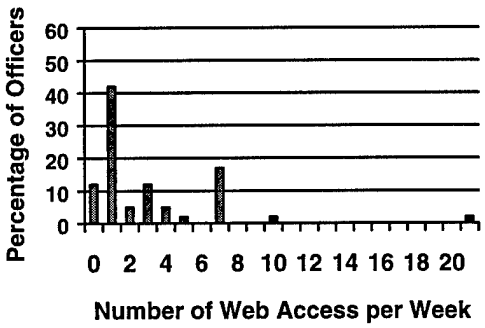
Within the Air Force, the use of the Web has grown phenomenally. The number of Air Force Web servers has grown from 100 to over 600 in just 6 months.[7] While experts disagree on the size and the growth of the internet, it can be assumed that the internet has *approximately* 100 percent annual growth[8].

The Internet User

There are several on-line surveys that attempt to determine the demographics of the typical internet, and Web in particular, user. In addition to the Research Survey conducted as part of this project, another comprehensive survey is performed regularly by Georgia Institute of Technology (GIT).[9] When the survey first started in January of 1994,[10] the average user was "primarily young and computer-savvy." Then the results jumped to older, more affluent users. The last survey shows that the average Web user age is coming down again and is about 33 years old. Each year more and more women use the internet. The last survey showed almost 30 percent of the users were woman. This figure has been steadily increasing over the last several years. The average income is $63,000 (US dollars) which is slightly down from the last survey ($69,000). Although many users are in college, most users (56 percent) are college graduates. Of significant interest is that security ranks as the number one concern in both the GIT poll and this project's Research Survey.

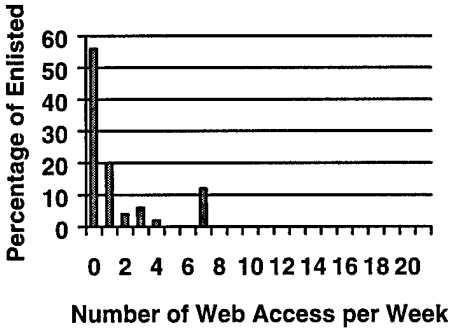
GIT found that 78 percent of the respondees use their Web browser daily. Air Force users have some catching up before they reach the usage that is common on the Web. The results of the Research Survey found that on the average, officers used their Web

browsers 3.4 times per week or about once every other day. Enlisted personnel use the Web even less, at 1.4 times per week (see appendix D for a summary of the Research Survey results). Just looking at averages does not tell the entire story in this case. Figure B-2 shows a histogram of Web use for officers surveyed. The figure shows that by far, the most common frequency of Web use is once a week. Figure B-3 shows similar data for the enlisted corps surveyed. This time the most common frequency of use is *no* times a week.



Source: Research Survey.

Figure B-2. Histogram of Officer Web Use per Week



Source: Research Survey.

Figure B-3. Histogram of Enlisted Corps Web Use per Week

Developmental Trends

There are several trends in the computer technology that indicate at least the *direction* the development of the technology is taking. The remainder of this section will highlight several of the trends that exist today. It is not intended to fully explain the trends, nor discuss how the trend specifically relates to the Air Force mission. These trends are intended just to indicate a rough idea of the direction that new developments are taking and the speed with which they are moving.

Java

As the general acceptance of the Web increases, new developments, such as Java,[11] accelerate the growth. Java is a programming language that makes it possible to run small applications remotely over a network, obviating the need for application software residing on the local hard drive.[12] Java applications, or "applets," can be simple spreadsheets or graphic-intensive bouncing balls and, as a function of Java, they'll work equally well regardless of the computer's operating system.[13] Incompatibility, the bane of computing, can become obsolete! There's even a basic level of security built in. Java checks each line of code before executing, making sure it's a legal command and using encryption tools to ensure the code hasn't been modified.[14] All-in-all, Java could result in a paradigm shift for the internet and the Web. At publication of this project, however, some Air Force bases have put a moratorium on the use of Java-enabled Web browser software.[15] Although Java has built-in protection from viruses, it seems as if the government is still cautious about downloading essentially executable files that have not been certified by the official procedures.

Proliferation of Home Pages

More and more private business and universities, as well as government organizations, are developing home pages for the Web. A Web home page is *de rigueur* for a corporation which doesn't want to fall behind in the business market. Not only are organizations developing home pages so "surfers" can visit them, individuals are beginning to post their own personal home pages. Personal home pages are no longer just the purview of the computer "geeks." Internet Service Providers (ISP) are now providing server space so that users can post their own home page. CompuServe allows users to

have up to one megabyte of storage space for pictures of themselves, hyperlinks to their favorite sites, or anything else they wish to put out for anyone with a modem and a computer to review.[16]

Intra-LAN Communication

Some private companies are not just using the internet and Web as a way to attract and communicate with external customers. They also recognize the importance of internal communications within the organization. Rather than setting up a self-contained corporate LAN, companies are beginning to take advantage of the potential of the internet and, through server management, use the internet as an "intra-net" to distribute information (even to geographically distant workers),[17] linking up with the world and enhancing corporate communications in one fell swoop. Some companies are beginning to shy away from expensive network operating system software and use common Web browser software to communicate on their "intra-net" *and* on their LAN.[18]

Multimedia

The Web is not just a visual interface. It is possible to transmit audio files via voice e-mail (e-mail messages which include a voice segment) or even radio broadcasts using RealAudio.[19] Live video (pictures *and* sound) can also be transmitted via the Web.[20] There are sites available on the Web that display digital photos of various places around the world. Detailed satellite imagery, which could distinguish individual cars in the Pentagon parking lot, is available on the Web.[21] Additionally, virtual reality is being introduced via Virtual Reality Modeling Language (VRML). VRML is used to create

three-dimensional interactive navigable "worlds."[22] Its usefulness for military operations and training is still being explored.

Encryption

The Web also has the potential to become the ultimate mail-order catalogue. The problem holding back the explosion of commerce on the Web has been security-related: how to assure customers that their credit card numbers are safe. Both IBM and Microsoft have been addressing that issue, competing to be the industry-standard. Currently, the Microsoft product appears to be proprietary. The IBM product, with its "open specification," is more attractive to developers.

Another potential encryption software candidate is Pretty Good Privacy (PGP).[23] PGP is a dual-key encryption methodology that is widely available. PGP users have a publicly-available key and a private key. The sender uses the receiver's public key to encrypt the message and the receiver decrypts the message using his private key. While PGP is not suitable for classified information, it is suitable for transmitting sensitive personal information.

Capacity and Bandwidth Improvements

In support of all these Web possibilities, hardware and connectivity have also developed and expanded. The commercial communications world is looking for ways to entice the bandwidth hungry consumer. Specifically, the telecommunications companies are finally in a position to offer standard telephone lines capable of merging data, voice and video into one homogeneous whole.

Another breakthrough makes even larger bandwidths possible. Asynchronous transfer mode (ATM) technology will send digitized information at more than 45,000 times the speed available on typical telephone lines.[24] ATM—putting voice, data, video, and image transmissions on the same line at a guaranteed bandwidth per channel—adds cable TV suppliers to the marketplace. Over the long term, competition will likely drive the cost of local and long-haul interconnectivity down.

Personal Digital Assistant (PDA)

All the information and opportunities on the Web can be overwhelming. One possible solution is a Personal Digital Assistant (PDA). In effect, a PDA knows your habits, favorite sites, and general preferences and uses this information to help you transition from just "surfing" the Web to really delving deeply and putting together the information in a useful way.[25]

Web Terminals

One result from such a shift could be a so-called "$500 machine," a terminal made of a keyboard, a processor, memory, and a network connection. Millions who can't afford a personal computer could gain access to opportunities currently beyond their reach. The stripped-down machines could populate any public space, in effect giving everybody ubiquitous access to the net.[26]

Unified Internet Account

Just as telephony seems to be developing towards one phone number per person, with that number staying with the person regardless of their location, people may have a single internet account with multiple uses (work and personal). People may carry their cellular

PDAs around with them just like some are carrying their cellular telephones with them now.

Notes

[1]*Webossary* [On-line]. Available CompuServe: GO www [1995, December 23].

[2]John Quarterman, "What is the Internet, Anyway?" *Matrix News*, 4(8), August 1994.

[3]Stephen Cobb, "Internet Firewalls," *Byte*, October 1995, 179.

[4]Darrel Beach, DDN Program Management Office, SSG/SINS, Gunter AFB, AL. personal interview with Maj Anne Marie Matonak, 14 February 1996.

[5]AFDIR 33-121, *Compendium of C4 Terminology*, Attachment 1, 5 July 1995, 126.

[6]Tim Stehle. *Getting Real About Usage Statistics* [On-line]. Available HTTP: http://www.infi.net/naa/stehle.html [1995, December 15].

[7]Beach.

[8]John S. Quarterman, "Internet Growth," *Matrix News*, 3(12), December 1993.

[9]"Consumer Survey of WWW Users, Preliminary Results from 4th Survey" (12 December 1995). [On-line]. Available HTTP: http://www.www.cc.gatech.edu/gvu/user_surveys/survey-04-1995 [1995, December 20].

[10]"Results from the First World Wide Web User Survey," (January 1994). [On-line]. Available HTTP: http://www.www.cc.gatech.edu/pitkow/survey/survey-1-1994/survey-paper.html [1996, March 7].

[11]"Java: Programming for the Internet." (1995). Sun Microsystems, Inc Mountain View, CA, http://JAVA.SUN.COM [1996, March 26].

[12]Robert Hertzbert, "Java Picks Up Steam," *WebWeek* 2, Issue 1, Jan 96.

[13]Philip Elmer-Dewitt, "Why Java is Hot," *Time*, 22 January 1996, 59.

[14]Ibid.

[15]Kris Krimmel (kkrimmel@sagate1.kelly.af.mil). (1996, February 28). Applet Enabled Browser Moratorium Issued at Kelly. E-mail to Multiple recipients of list <www@infosphere.safb.af.mil>.

[16]"Personal Home Page Publishing Service." CompuServe. [On-line]. Available HTTP: http://ourworld.compuserve.com [1996, February 12].

[17]Groupware or Webware? (*Wall Street Journal,* 7 November 1995, A1). [On-line]. Available via Edupage List: listproc@elanor.oit.unc.edu [1995, November].

[18]Mr. Charles Hall, Systems Engineer, Silicon Graphics Corporation. Briefing to ACSC Students, 13 December 1995.

[19]"RealAudio, Audio-on-demand for the Internet" (22 March 1996), Progressive Networks, Seattle WA [On-line]. Available HTTP: http://www.realaudio.com. [1996, March 26].

[20]Mark Dery, "uplist," *VirtualCity* 1, Issue 2 (Winter 1996): 5.

[21]Daniel Burstein. (1992). Photography from Orbit. In *The Risks Digest* (Vol 14, Issue 6, [On-line]. Available HTTP: http://catless.ncl.ac.uk/Risks/14.06.html [1996, April 12].

Notes

[22]Dave Blackburn, "Get out your 3D Glasses," *VirtualCity* 1, Issue 2 (Winter 1996): 20.

[23]"Pretty Good Privacy (PGP)." [On-line] Available HTTP: http://web.mit.edu/network/pgp.html.

[24]AFDIR 33-121.

[25]This Is The Web—It's Not A Reading Room. (*Washington Post,* 12 November 1995, C5), and "Delphi Strives for Mass Intimacy." (*Business Week*, 16 October 1995, 74). [On-line]. Available via Edupage List: listproc@elanor.oit.unc.edu [1995].

[26]Joshua Cooper Ramos, "How Cheap Can Computers Get?" *Time*, 22 January 1996, 60.

Appendix C

Internet History

There are many sources available outlining the history of the internet. There are books, magazine articles, and on-line sources with good descriptions of internet history. The following summary was drawn from several primary sources.[1] However, the information is supplemented by several other sources (referenced by exception) for additional perspective.

Summary

There is very little debate that the origins of the internet were with the Advanced Research Projects Agency (ARPA). ARPA was formed in 1957 in response to the USSR's launch of Sputnik. ARPA was established as the US lead in science and technology applicable to the military. The DOD commissioned ARPANET in 1969 as a test network that was decentralized so that messages could be rerouted in the event that part of the communications system was destroyed by nuclear attack. The ARPANET gradually grew by adding new computers and users at government and university sites. From the mid-1970s to the 1980s, smaller networks that used the ARPANET technology added to the number of sites available on the "internetwork."[2]

In 1983, ARPA divided the network into ARPANET for research and MILNET for military applications. Academia became more and more significant in the internet when the National Science Federation established NSFNET for scholarly research (1986). NSFNET soon became the backbone of the internet. Finally, in 1990, ARPA bowed out and decommissioned the ARPANET.

More and more countries became connected to the NSFNET through their own intra-country networks. Several services or applications were developed for easier communication on the internet. The more popular services are telnet, FTP, and HTTP (Web). The Web is the current pinnacle of connectivity technology. The Web was first released in 1992 by Corporation for Research and Education Networking (CREN). The first popular Web browser was written by the National Center for Supercomputing Applications (NCSA) in Champaign, Illinois and released in 1993. In addition to the growing number of local on-line services, traditional nationwide on-line internet services providers (ISP) (CompuServe, America Online, and Prodigy) began to provide internet and Web access in 1995. Also in 1995, the NSFNET reverted back to a research network and the main US backbone traffic began to be rerouted through interconnected network providers.

The United States government has become more and more connected. The White House,[3] Library of Congress,[4] and IRS[5] have their own Web home pages. Several acts have been passed which increase the stature of this communication trend. Some of these acts and bills include the National Information Infrastructure Act in 1993 and the controversial Telecommunications Bill of 1996.[6] Although the government is becoming more and more connected, there are still examples of not everyone fully embracing the

paradigm shift. Recently a reporter, whose work is solely on-line, was denied access to the business club run by and for working White House journalists. Gallery officials said he failed to meet the qualifications of a working journalist.[7]

An interesting survey of the internet through the late 1980s can be found in the book *The Cuckoo's Egg*, written by Clifford Stoll.[8] Stoll was an unfunded astro-physicist working as a network administrator for the University of California at Berkeley. Because of a $0.75 accounting error in computer time charging, he almost single-handedly tracked down a German "cracker" (a malicious hacker) group who had infiltrated numerous US computer facilities. The group had capitalized on the openness of the university environment and the known security holes in the UNIX operating system to gain access to Stoll's computers. From these computers, the crackers gained access to numerous other computer networks across the US and in other parts of the world. Many of the computer networks that were broken into were government and military networks.

Chronological Summary

1962 Paul Baran from RAND designed a packet-switching network to survive nuclear attack. Messages are broken down into units of equal size, routed along a functional path, then reassembled at the destination.

1965 ARPA sponsored a study on "cooperative network of time-sharing computers."

1967 First design paper on ARPANET published by Lawrence G. Roberts.

1969 DOD commissioned the ARPANET, a decentralized network built so that messages could be rerouted in the event that part of the communications system was destroyed by nuclear attack. Nodes are connected at UCLA, Stanford Research Institute, and University of Utah.

1971 15 host computers are on the ARPANET.

1972 First e-mail program is written to send messages across distributed networks.

1972 ALOHANET (University of Hawaii) is connected to ARPANET.

1973 First international ARPANET connections are established to the University College of London (England) and Royal Radar Establishment (Norway).

First telnet service established.

1975 Operational management of ARPANET transferred to DCA (Defense Communications Agency, now Defense Information Systems Agency (DISA)).

1976 Elizabeth, Queen of United Kingdom, sends out an e-mail.

1979 USENET originates at Duke University and the University of North Carolina.

ARPA establishes the Internet Configuration Control Board (ICCB).

1981 BITNET ("Because It's Time NETwork) established as a network at City University of New York and has first connection with Yale. BITNET offers a method for scholarly discussion for academics not involved in the sciences.

DOD declares Transmission Control Protocol/Internet Protocol (TCP/IP) suite to be standard for DOD.

EUNET (Europe Unix Network) is created to provide e-mail and SUENET services, original connections between the Netherlands, Denmark, Sweden, and UK.

Computer and Science Network (CSNET) established through seed money granted by NSF to provide networking services (especially e-mail) to university scientists with no access to ARPANET.

1982 External Gateway Protocol (EGP) specification established. EGP is used for gateways between networks.

1983 ARPANET splits into ARPANET for research and MILNET for military applications. TCP/IP, computer code for communication with the internet, is developed at the University of California, funded by ARPA.

CSNET and ARPANET gateway put in place.

Name server developed at University of Wisconsin, no longer requiring users to know the exact path to other systems.

Internet Activities Board (IAB) established, replaces ICCB.

European Academic and Research Network (EARN) established. Very similar to the way BITNET works with a gateway funded by IBM.

FIDONET developed by Tom Jennings.

1984 JUNET (Japan Unix Network) established.

Domain Name Server (DNS) introduced.

Joint Academic Network (JANET) established in United Kingdom.

Moderated newsgroups introduced on USENET.

1986 National Science Foundation Network (NSFNET) established to connect 5 supercomputer centers for scholarly research. This network becomes the initial internet backbone with a speed of 56Kbps.

Mail Exchanger (MX) records developed by Craig Partridge allows non-IP network hosts to have domain addresses.

Bay Area Regional Research Network (BARRNET) established.

1987 NSF signs contracts with IBM, MCI, and Merit Network Inc., to manage and upgrade NSFNET.

1988 NSFNET backbone upgraded to "T-1" standard (1.544 Mega bits per second (Mbps)).

Los Nettos Network created with no federal funding, instead supported by regional members.

California Education and Research Federation Network (CERFNET) established.

Internet "worm" or virus "burrows" through internet affecting approximately 6,000 of the 60,000 hosts (1 November).

Computer Emergency Response Team (CERT) is formed by DARPA (formerly ARPA) in response to needs exhibited during a internet-wide "worm" incident from earlier in the year. The CERT Coordination Center (CERT/CC) is located at Carnegie Mellon University's Software Engineering Institute and serves as a focal point for response to internet computer security problems.[9]

Countries connected to NSFNET: Canada, Denmark, Finland, France, Iceland, Norway, Sweden.

1989 Reseaux IP Europeans (RIPE) formed by European internet providers to ensure the necessary administrative and technical coordination to allow operation of the pan-European IP Network.

First project proposal for Web written and circulated for comments at Corporation for Research and Education Networking (CREN).

First relays between commercial e-mail carrier and the internet: MCI Mail through the Corporation for the National Research Initiative (CNRI), and CompuServe through Ohio State University.

CREN is formed by the merge of CSNet and BITNET.

Australian Academic Research Network (AARNET) established.

Archie developed by staff and students at McGill University in Quebec to help keep track of free software from anonymous FTP sites.

Countries connected to NSFNET: Australia, Germany, Israel, Italy, Japan, Mexico, Netherlands, New Zealand, Puerto Rico, UK.

Cuckoo's Egg is written by Clifford Stoll. The book tells of a real-life tale of Stoll tracking down a German "cracker" group who infiltrated numerous US computer facilities. [10]

1990 ARPANET decommissioned.

Initial Web prototype is developed by CERN, European Particle Physics Laboratory in Switzerland. It allows user to browse and select links that bring text, graphics, audio, or video on screen.

"The World" comes on-line as the first commercial provider of internet dial-up access.

CA*NET is formed by 10 regional networks as Canadian backbone with direct connection to NSFNET.

Countries connecting to NSFNET: Argentina, Austria, Belgium, Brazil, Chile, Greece, India, Ireland, South Korea, Spain, Switzerland.

1991 Gopher is developed at the University of Minnesota to help the campus community find answers to computer related questions.

Web is released on CERN machines.

NSF lifts restrictions against commercial use of the internet.

Pretty Good Privacy (PGP) encryption software released by Philip Zimmerman.

WAIS invented by Brester Kahle.

President George Bush signs into law the High Performance Computing Act providing $650 million in new spending by the NSF, $388 million by DARPA (formerly ARPA), and $31 million by the Department of Commerce's National

Institute of Standards and Technology. This Act establishes the National Research and Education Network (NREN).

NSFNET backbone upgraded to "T-3" standard (44.736 Mbps).

Countries connecting to NSFNET: Croatia, Czech Republic, Hong Kong, Hungary, Poland, Portugal, Singapore, South Africa, Taiwan, Tunisia.

1992 Web released by CERN.

Veronica is released by University of Nevada.

World Bank comes on-line.

President Bill Clinton announces plans to develop a national electronic infrastructure through government and private efforts, with most government support going to the National Research and Education Network (NREN).

Countries connecting to NSFNET: Cameroon, Cyprus, Ecuador, Estonia, Kuwait, Latvia, Luxembourg, Malaysia, Slovakia, Slovenia, Thailand, Venezuela.

1993 President Bill Clinton signs the Government Printing Office Electronic Access Act to provide on-line access of federal documents, including the Federal Register, the Congressional Record, and other sources distributed through the Government Printing Office. United States White House comes on-line.[11]

The National Information Infrastructure Act is introduced into the House of Representatives and passes. Its companion bill, the National Competitive Act, is introduced into the Senate. The Senate bill is designed to update the High Performance Computing Act of 1991 by focusing on the provision of applications rather than on high-speed networks.

InterNIC created by NSF to provide specific internet services.

The Web browser *Mosaic* is released in February by the National Center for Supercomputing Applications (NCSA) in Champaign, Illinois. It allows use of Web to browse and click or select links that bring text, graphics, audio, or video to the screen.

By March, Web traffic represents 0.1 percent of NSF backbone traffic.

By September, Web traffic represents 1 percent of NSF backbone traffic.

By October, there are over 200 known Web servers.

The White House receives e-mail connections.

The White House announces the formation of the National Information Infrastructure Testbed, an industry and government coalition to develop applications for the internet, including remote research collaboration and medical consulting.

Web proliferates at a 341,634 percent annual growth rate of service traffic. Gopher's growth is 997 percent.

Countries connecting to NSFNET: Bulgaria, Costa Rica, Egypt, Fiji, Ghana, Guam, Indonesia, Kazakhstan, Kenya, Liechtenstein, Peru, Romania, Russian Federation, Turkey, Ukraine, UAE, Virgin Islands.

1994 United States Senate and House provide on-line information servers.

Vice-President Gore conducts computer-based news conference from the White House.

The White House puts home page, "An Interactive Citizen's Handbook," on the Web. Includes information on the First Family, agencies and commissions of the Executive Branch, White House electronic publications, and virtual tours of the White House, the Old Executive Office, and the First Ladies Garden.[12]

The National Competitive Act is approved by Senate.

Non-secure Internet Protocol Network (NIPRNET) begins coming on-line. NIPRNET is intended to eventually replace MILNET.[13]

Japanese Prime Minister [http://www.kantei.go.hp], UK's HM Treasury [http://www.hm-treasury.gov.uk], and New Zealand's Info Tech Prime Minister [http://www.govt.nz/] on-line.

Netscape, a Web browser is introduced by Mosaic Communications Corporation (later changes its name to Netscape Communications Corporation).

Web edges out telnet to become second most popular internet service (behind FTP) based on percent of packets and bytes traffic distributed on NSFNET.

Trans-European Research and Education Network Association (TERENA) is formed by the merge of RARE and EARN, with representatives from 38 countries as well as CERN and ECMWF. TERERNA's aim is to "promote and participate in the development of a high quality international information and telecommunications infrastructure for the benefit of research and education."

Countries connecting to NSFNET: Algeria, Armenia, Bermuda, Burkina Faso, China, Colombia, French Polynesia, Jamaica, Lebanon, Lithuania, Macao, Morocco, New Caledonia, Nicaragua, Niger, Panama, Philippines, Senegal, Sri Lanka, Swaziland, Uruguay, Uzbekistan.

1995 NSFNET reverts back to research network. Main US backbone traffic is now routed through interconnected network providers.

Hong Kong police disconnect all but one of the colonies internet providers in search of a hacker. 10,000 people are left without internet access.

Traditional on-line internet services providers (ISP) (CompuServe, America Online, and Prodigy) begin to provide internet access.

Web surpasses FTP as service with the greatest amount traffic on NSFNET (based on packet and byte count).

1996 CompuServe begins to offer new Parental Controls to restrict access to "sites" that may contain adult-oriented content. CompuServe also discontinues suspension of global access to more than 200 Newsgroups recently suspended in response to an investigation by the prosecutor's office in Munich Germany.[14]

President Clinton signs into law new telecommunications bill. This bill revamps the 1934 Communications Act. It will let local long-distance phone companies and cable companies into each others' businesses, deregulate cable rates, and allow media companies to expand their holdings more easily. The Communications Decency Act, part of the bill, will also, for the first time, outlaw the transmission of indecent and other sexually explicit materials to minors over computer networks. It will give parents a new tool to "zap" from their TV sets shows electronically rated for violent and other objectionable content. The provision will require new TV sets be equipped with a special computer chip to make this work. President Clinton signed the bill at the Library of Congress first in ink and then with an "electronic pen" on an electronic tablet.[15]

New telecommunications bill under attack immediately upon signing by groups opposing the computer "censorship" provision. Some of these groups include: the National Abortion and Reproductive Rights Action League, the American Civil Liberties Union, Planned Parenthood, abortion rights groups, CompuServe, Apple Computer Inc., Microsoft Corp., America Online, the American Library Association, the Society of Professional Journalists, and others. Less than a week after President Clinton signed the bill, a federal judge issued a temporary restraining order to prevent the government from enforcing the new law.[16]

The day after President Clinton signed new telecommunications bill, many Web sites protested the Communications Decency Act. The protesters changed the background color of their Web "sites" to black. In addition to sites that deal with the explicit graphics, many "main stream" sites[17] joined in and protested the "censorship" aspect of the bill. [18]

> AT&T announces it will offer telephone customers five hours of free internet access each month for a year, bringing computer network service a step closer to becoming a utility like electricity.[19]

History of Computer Security Risks

The risks associated with computers have changed and grown with the manner in which they are used and networked. Traditional un-networked computer security risks have centered around the loss of data due to operator error, computer viruses, loss of data due to natural disaster, and, in rare cases, theft or intentional destruction of computer files by a disgruntled employee or former employee. All of these risks were handled by controlling access to *individual* computers. Password protection, screening floppies for viruses, or simply keeping computers with sensitive information behind locked doors mitigated much of the risks.

LANs provided a new wrinkle to the computer security problem. Direct physical access to a computer was no longer necessary for gaining access to its files. An individual armed with the right information just required access to any computer on the local network. This situation was initially not all that alarming because typically most users on a local network are employees or members of the organization. Access to each *individual* LAN was required. Diligent password protection and supervision prevented most problems. Access to an organization's computers was regulated to some degree and malicious users were rare.

The internet introduced the next step in the evolution of computer security problem. When an organization connects to the internet, the number of users that can access or attempt to access their computers is *unlimited.* The general philosophy of the internet is

to provide open access of information to all users. While most users are merely going about their own business, there is an element which is more interested in illegally penetrating other computer systems for fun, profit, or mischief. The internet hackers are a significant new threat because of their dedication to hacking, their sophistication, and their ability to share information. If an organization's computers are only hooked up to a local network, the organization has to consider the possibility of a mischievous hacker, but when the organization hooks up to the internet the organization can be assured that it will eventually be "hacked."

The biggest problem to the Air Force is not the "cracker" breaking into classified networks. The biggest problem is unauthorized intrusion into unclassified networks. Attempts to break into the government LANs abound. On 28 February 1994, a US magistrate judge authorized government agents to seize computer equipment from three residences around Wright-Patterson Air Force Base, Ohio. The suspects were all between the ages of 18 and 24. According to military investigators, the hackers placed illegal telephone calls to the 645th Communications-Computer Systems Group and logged onto the military computer network. They then used stolen passwords to log onto the internet. The agents had received an anonymous tip that a base telephone number was being passed among hackers and had been posted on a local computer bulletin board.[20]

Government networks tend to have an abundance of instructions, policies, and hardware designed to keep the unauthorized user out. The easiest way to prevent unauthorized users from breaking into classified , or even unclassified, networks is to not connect them to any other network or only connect via specially designed "firewalls." A firewall is a dedicated computer or router with special software that sits between the

internet and the LAN. The firewall is used to implement the policy and enforce service and user access restriction. The firewall blocks and monitors transmissions going back and forth between the internet and the LAN.[21] No information systems carrying classified data are connected to the internet, and no classified networks have been breached by hackers, according to Chris Goggans, president of Computer Security Technologies.[22]

In November of 1988, a "worm" created by Robert Tappan Morris was released on the internet and rapidly brought the internet to its knees as it penetrated over 6,000 computers. The internet worm penetrated UNIX servers on the internet and began duplicating itself. In 1995, an automated hacking program named Security Administrator's Tool for Analyzing Networks (SATAN),[23] was released on the internet amid cries that this foreshadowed the end of the internet. SATAN and Morris's worm share common characteristics in that they primarily targeted UNIX operating systems and known holes in UNIX systems.

UNIX has historically been the operating system of choice for most internet computers. It was developed originally by AT&T's Bell Labs where it was a loosely structured cooperative venture between Bell Labs and universities.[24] UNIX source code was widely distributed and available to anyone. When UNIX was initially being developed, no one gave serious consideration to security. The result is an operating system that has many security holes in it.

Because UNIX is the most widely used operating system on the internet, it has born the brunt of hacker attacks. Fortunately, most of the UNIX bugs are known and fixes are available. A properly installed UNIX operating system with a firewall can actually be a quite secure operating system.[25] Unfortunately many computers running UNIX are

continually breached because the system operators are still running old versions of UNIX, or they have not fixed known bugs with available patches.

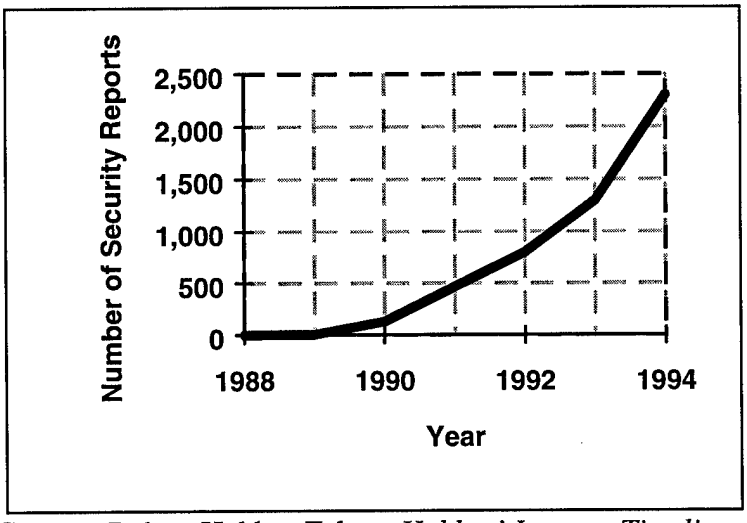
A good way to test the security of a UNIX operating system is to attack it with the automated hacking program SATAN. As a matter of fact, SATAN was designed for that very purpose. Contrary to the cries of doom and devastation when SATAN was initially released, it was intended to assist system operators to determine how secure their operating systems were. SATAN contains the majority of *known* hacking techniques that are widely available on the internet. Unfortunately by hacking standards, SATAN is old and outdated. Today, if SATAN can penetrate your system, just about any hacker can.

Besides penetrating operating systems by exploiting known bugs in the software, hackers are also adept at cracking passwords. There are numerous programs on the internet that run through dictionaries and lists of common names to search out passwords. Using these techniques, Robert Morris compiled a list of over 400 user IDs and passwords in just over four months prior to releasing his internet worm.[26] Another common technique for obtaining passwords is for hackers to upload and run programs called "sniffers" onto a system. These programs reside and watch for users logging in and then capture their passwords. Once a hacker has a user's username and password they can log directly on to a network with all of the privileges granted to that user.

In 1988, Defense Advanced Research Projects Agency (DARPA) formed the Computer Emergency Response Team (CERT) in response to needs exhibited during the internet wide Robert Morris "worm" incident. The CERT Coordination Center is located at Carnegie Mellon University's Software Engineering Institute and serves as a focal point for response to internet computer security problems.[27] CERT regularly publishes

reports at their FTP site[28] describing computer security incidents. For example, this site lists well over 100 pages of known UNIX bugs and potential fixes or workarounds.

The number of security intrusion incidents, or unwanted attempts into computer networks, *reported* to the Computer Emergency Response Team (CERT) has risen from 130 in 1990 to 2300 in 1994 (figure C-1). Most of these incidents are not from "kids getting their kicks with modems," but rather, are systematic and automated probing of new internet connections. Computer crackers gained unauthorized access through the internet in more than 80 percent of the computer crimes investigated by the FBI.[29] The DOD is particularly concerned about this growing trend. Attacks against DOD computer systems are doubling every year and more than 500 attacks on defense information systems were expected by the end of 1995.[30]



Source: Robert Hobbes Zakon. *Hobbes' Internet Timeline, v2.2*, http://info.isoc.org/guest/zakon/Internet/History/HIT.html. 14 Dec 1995.

Figure C-1. Number of CERT Security Reports

According to *Network Security Secrets*, the average hacker is between 14 and 21 years old, in high school or college, very bright, and, of course, loves computers. For the

most part, hackers operate without malice. It is estimated that only 1 percent of all hackers actually engage in destructive or fraudulent activity,[31] these malicious hackers are often referred to as "crackers."

Hackers share their techniques and information on underground bulletin boards. Sometimes they just brag about their feats of computer prowess, but sometimes they pass copies of credit card numbers, stolen telephone codes, and other things. The underground bulletin board systems (BBS) provide schematics for telephone "blueboxes" or patch panels, pirated software, programs for breaking into systems, and other obnoxious material. Operation Sundevil, in May 1990, was a nationwide campaign that specifically targeted underground BBSs. Operation Sundevil seized 25 BBSs by raiding homes and confiscating computer equipment used to run the boards. One feature of hackers that was illustrated in Operation Sundevil is that hackers cannot keep quiet about their conquests and techniques. Once a hacker makes a successful penetration or develops a new technique, it is quickly promulgated across the underground bulletin boards with lists of susceptible computers.[32]

Although most hackers gain the information and code that they need from underground bulletin boards, there are some hackers, like Kevin Mitnick, who obtain code and passwords directly from the source. Mitnick obtained code by what hackers refer to as "social engineering," which is impersonating supervisors, impersonating telephone linemen, searching trashcans, and other means. The ease with which Mitnick obtained critical information from government agencies, telephone companies, and software vendors is astounding.[33]

Hackers can also "spoof" the Internet Protocol (IP) addresses. The IP addresses are used by internet computers to authenticate users. Hackers trick routers into making false or improper connections by emulating other IP addresses or taking advantage of IP address protocols which permit automatic re-routing of messages when a path is clogged or temporarily down. For instance, all Air Force IP addresses end in ".af.mil." A hacker can either emulate an ".af.mil" IP address or, more likely, gain access to an open ".af.mil" computer and access other ".af.mil" addresses from the first ".af.mil" IP address. The infamous German cracker group uncovered by Clifford Stoll in late 1980s used this IP spoofing technique to gain access to numerous government computer systems after exploiting a security hole in the UNIX operating system of the University of California at Berkeley computer network.[34]

The widespread availability of free and easily accessible software on the internet makes the possibility of "Trojan horses" or "trap doors" a real problem. A Trojan horse or trap door is written into the actual program code. When the Trojan horse software is uploaded and run on an unsuspecting user's computer, the software writer can trigger the Trojan horse to gain access to the user's computer. A widely-vailable and popular free file transfer protocol (FTP) program for running an FTP site was discovered to contain just such a Trojan horse.[35] It was an ideal vehicle for a Trojan horse because the FTP program ran continually on the unsuspecting host computer, infecting the remote computers that connected to it.

Although security is a significant concern, the answer to the majority of DOD unclassified networks is not to "unplug" them and make them impenetrable from the outside. There are several reasons for this. First, not all security problems come from

outside of networks. Often an authorized network user can create security problems (either intentionally or often unintentionally). Second, and perhaps more importantly for most unclassified networks, the whole point of the network is accessibility to users. These users can be base personnel logging on to the base home page, Air University students checking their e-mail from home, or even interested civilians trying to learn more about the Air Force by visiting Air Force computer sites.

Notes

[1]Kristin Jacobsen, "Time To Put the Internet in Perspective", *C&RL News*, Mar 1995, p144-147, and Robert Hobbes Zakon. *Hobbes' Internet Timeline, v2.2* [On-line]. Available HTTP: http://info.isoc.org/guest/zakon/Internet/History/HIT.html. 14 December 1995. (also available by automatic e-mail reply to <timeline@hobbes.mitre.org>) and http://www.w3.org/pub/WWW/.

[2]Lt Col George Kaliwai III. "Surfing the Third Wave." Prepared for completion of National Defense Fellowship, Ohio State University, July 1994, 5.

[3]"White House Home Page." [On-line]. Available HTTP: http://www1.whitehouse.gov/WH/ welcome.html [1996, February 17].

[4]"Library of Congress Home Page." [On-line]. Available HTTP: http://www.loc.gov [1996, February 17].

[5]"Internal Revenue Service Home Page." [On-line]. Available HTTP: http://www.irs.ustreas.gov [1996, January 15].

[6]"CNN Interactive." [On-line]. Available HTTP: http://www.cnn.com [1996, February 9].

[7]"Determining the Status of Cyberjournalists in Washington." (1996, February 26), *New York TimesFax Internet edition*, [On-line]. Available HTTP: http://nytimesfax.com, page 6.

[8]Stoll, Clifford, *The Cuckoo's Egg*, New York, NY: Doubleday, 1989.

[9]Richard D. Pethia, Kenneth R. van Wyk, *Computer Emergency Response - An International Problem*, Pittsburg, PA: Computer Emergency Response Team/Coordination Center, Software Engineering Institute Carnegie Mellon University, Pittsburgh, PA, 14 November 1990. [On-line]. Available HTTP: http://www.riken.jo.jp/ archieves/security/cert/info/security.response.cert.txt, 28 February 1996.

[10]Stoll.

[11]"White House Home Page."

[12]Ibid.

[13]Darrel Beach, DDN Program Management Office, SSG/SINS, Gunter AFB, AL. personal interview with Maj Anne Marie Matonak, 14 February 1996.

[14]"Parental Controls." [On-line] Available CompuServe: GO Controls [1996, February 13].

Notes

[15]"CNN Interactive." [1996, February 9].

[16]"CNN Interactive." [1996, February 9] and Andrews, Edmund L., (1996, February 9), Communications Law Triggers Lawsuits. *New York TimesFax Internet Edition*, [On-line], p1 (6 paragraphs). Available: HTTP: http://nytimesfax.com/ [1996, February 9] and What's New. [On-line]. Available Compuserve: GO Telecom [1996, February 27].

[17]"Yahoo Home Page." [On-line]. Available HTTP: http://www.yahoo.com [1996, February 9].

[18]"CNN Interactive." [1996, February 9].

[19]Peter H. Lewis (1996, February 28). "AT&T Unveils Ambitions Internet Plan." *New York TimesFax Internet Edition* [On-line]. Available HTTP: http://nytimesfax.com/.

[20]Bobbie Mixon, ASC Public Affairs, "Agents seize computers, suspect hacking," *Skywrighter,* 4 March 1994: 1.

[21]NIST Special Pub 800-10. National Institute of Standards and Technology. [On-line]. Available HTTP: http://csrc.ncsl.nist.gov/nistpubs/800-10/ [1996, January 17].

[22]Pat Cooper, "Computer Hackers Beware," *Air Force Times*, 2 October 95, 32.

[23]Wietse Venema and Dan Farmer [1995, April 24], *Security Administrator's Tool for Analyzing Networks* [On-line]. Available HTTP: http//www.fish.com/satan/ [1996, March 16].

[24]David J. Stang and Sylvia Moon, *Network Security Secrets*, IDG Books Worldwide Inc, San Mateo CA, 1993.

[25]Stang and Moon, 743.

[26]Stang and Moon, 735.

[27]Pethia and van Wyk.

[28]CERT Coordination Center FTP Server, public directory. Pittsburg, PA: Computer Emergency Response Team/Coordination Center, Software Engineering Institute Carnegie Mellon University, Pittsburgh, PA, (no date). [On-line]. Available FTP: ftp://cert.org/pub [1996, March 15].

[29]Stephen Cobb, "Internet Firewalls," *Byte*, October 1995, 179.

[30]Cooper.

[31]Stang and Moon, 199-200.

[32]Bruce Sterling. *The Hacker Crackdown* [On-line]. Available: HTTP: http://www.eecs.nwu.edu/hacker_crackdown/ [1996, January 15].

[33]Tsutomu Shimomura and John Markoff. "Catching Kevin," *Wired*, February 1996, 120.

[34]Stoll.

[35]Stang and Moon, 200.

Appendix D

Research Survey Summary

The following survey was designed to establish Air Force internet user concerns and preferences in order to sculpt an overall policy that ultimately had the "customer" in mind. The composition of the surveyed population was planned to be as representative as possible of the overall Air Force user population. The population targeted was composed of civilian, enlisted, and officer members of Professional Military Education (PME) schools located in Montgomery, Alabama. The PME school populations are composed of a variety of specialties from locations across the globe. For these reasons, the research team believed that, for the scope of this study, the population surveyed comprised a valid cross-section. The final tally included 7 civilians, 51 enlisted, and 41 officers.

A sample survey is included in this appendix. Table D-1 summarizes the Research Survey results. Table D-2 summarizes the most important contribution of the internet, while table D-3 summarizes the most annoying aspect of the internet. Table D-4 summarizes the types of un-solicited e-mail. Raw data is archived and available from ACSC/DR.

Your Air Force Internet

Student Research Survey for ACSC Project 96-007

The Air Force does not currently have a comprehensive policy for the use of the internet and world wide web. ACSC student research team 96-007 is formulating just such a policy for submission to the USAF leadership. This survey is *your* chance to be heard during the creation of a policy that could have long term effects on how *you* are directed to use the internet of the future. Please take five minutes of your time to give us your thoughts so that we may produce a more balanced, user-friendly proposal. In return, we'll be glad to send an executive summary of the final report to the location you annotate at the end of this form. NOTE: You may continue any answer in the margin or by attaching a separate page.

Your Background

Name (optional)_____ Rank____ Primary specialty_____

Service Component_____ (USAF,USN,IO, . . . etc.)

Do you . . .
own a computer? Yes / No
have a **private** (home) internet access account? Yes / No
ever use File Transfer Protocol (ftp) functions? Yes / No If Yes, how often_____
ever use Telnet functions? Yes / No If Yes, how often_____
access the worldwide web from work roughly once a day / once a week / ___ times a wk.

1. What do you feel is the most important contribution of the Internet to the Air Force Mission? _____

2. What do feel is the most annoying aspect of the internet in Air Force use, if any?
_____

3. In the following list of Internet usage issues, **circle** the response that characterizes the importance that **you** give to the particular issue, 1 being not important and 5 being very important. [Expand your answer in the margin or by attachment, if desired]

3.1 Privacy:		1	2	3	4	5
3.2 Security:		1	2	3	4	5
3.3 Decency:	1	2	3	4	5	
3.4 Copyrights:		1	2	3	4	5

3.5 Home access to work system:	1	2	3	4	5
3.6 Official use restrictions:	1	2	3	4	5
3.7 Local help desk:	1	2	3	4	5
3.8 Official e-mail from work:	1	2	3	4	5
3.9 Personal e-mail from work:	1	2	3	4	5

4. In the following list of e-mail "types," **circle the number** under the column that most closely characterizes your feelings about receiving an **unsolicited** message in your e-mail inbox.

	Always Proper	Sometimes Proper	Never Proper
4.1 A fellow worker's message to you:	1	2	3
4.2 A fellow worker's message to everyone:	1	2	3
4.3 System outage bulletins:	1	2	3
4.4 Solicitation for a charitable activity:	1	2	3
4.5 Announcement of an on-base function:	1	2	3
4.6 Volunteer request for additional duty:	1	2	3
4.7 Real estate offer for military members:	1	2	3
4.8 Greeting based on a religious holiday:	1	2	3
4.9 Humor sent to everyone:	1	2	3

5. In addition to items you may have marked above, what other types of unsolicited e-mail have you received that you **did not** want to receive?

_____

6. Have you ever had a "personal" e-mail message forwarded to others without your consent in a manner that embarrassed or upset you? Yes / No

7. Location to deliver executive summary of research (if desired)_____

Thank You!

Table D-1. Research Survey Summary

Question from Survey	All Cats	Stand Dev	Officer	Enlisted	Civilian
Own Computer?	81%		93%	76%	43%
Private Inet Access?	39%		65%	24%	0%
FTP ever?	35%		49%	26%	14%
FTP/week	2.3	1.93	0.5	2.8	0.0
Telnet?	23%		22%	28%	0%
Telnet/week	3.5	3.96	1.0	4.4	0.0
Web access/week	2.2	3.14	3.4	1.4	0.9
1. Most important contribution	See matrix				
2. Most annoying	See matrix				
3.0 Importance of the following issues (5 highest)					
3.1 Privacy	3.9	1.28	3.8	4.0	4.0
3.2 Security	4.3	1.22	4.5	4.3	3.4
3.3 Decency	3.7	1.22	3.5	3.8	4.3
3.4 Copyrights	3.2	1.27	2.9	3.5	3.7
3.5 Home access	3.8	1.05	4.0	3.8	3.0
3.6 Official Use	3.6	1.00	3.5	3.7	3.6
3.7 Help Desk	3.5	1.04	3.4	3.6	3.1
3.8 Official E-mail	4.3	1.06	4.2	4.4	3.7
3.9 Personal E-mail	3.1	1.29	3.4	3.0	2.9
4.0 "Properness" of the following e-mails (1 is most)					
4.1 Worker's message to you	1.4	0.51	1.3	1.5	1.6
4.2 Worker's message to everyone	1.8	0.51	2.0	1.7	1.6
4.3 System outage bulletins	1.2	0.43	1.3	1.2	1.0
4.4 Solicitation for a charitable activity	2.4	0.59	2.6	2.3	2.3
4.5 Announcement of on-base function	1.7	0.52	1.8	1.6	1.7
4.6 Volunteer request for additional duty:	1.8	0.58	1.9	1.7	1.6
4.7 Real estate offer for military members	2.8	0.50	2.9	2.7	2.4
4.8 Greeting based on a religious holiday	2.4	0.66	2.2	2.6	2.1
4.9 Humor sent to everyone	2.4	0.56	2.4	2.4	2.0
5. Unsolicited e-mails	See matrix				
6. Embarrassing forward of e-mail	5.5%		10%	2%	0%
7. Request Executive summary?	17		8	8	1

Table D-2. Research Survey Summary, Most Important Aspect of Internet

***Access* 22**			
Access to information	15	Easy access to information	1
Access to international information	3	24 hour access	1
Library access	1	Easier access to overseas personnel	1
***Information* 40**			
Speed of receipt of Information	17	Diversity of information at fingertips	2
Information sharing via e-mail and Web	15	Speedy outflow of information	1
Volume of information	5		
***Connectivity* 7**			
Connectivity	1	Forum capability	1
Supports Total Force: able to communicate with Active Duty	1	Easy off-duty communications with USAF folks	2
Being reachable from anywhere	2		
***Miscellaneous Benefits* 5**			
Provides accountability and accuracy	1	Focused information from TOP of command chain	2
No paper trail	1	Paperless environment	1
***Communication* 19**			
Rapid communication	2	Free mail	1
Communication	2	E-mail	9
Effective alternate communication between non-collocated organizations	3	Allows immediate delivery of important message	1
		Reduces incoming telephone calls	1
***Specific Services* 19**			
Quick changes to regulations, TOs, AFIs	1	Information on specific bases and services	1
Assignment advertising	2	Current AF news	3
Career field crossflow of information	1	Research/technical	6
Distribution of reports and articles	2	Public affairs information	1
Good news	1	Current Pentagon information	1
***No Important Contribution* 2**			

Table D-3. Research Survey Summary, Most Annoying Aspect of Internet

Performance 15			
Lack of equipment capability (modem)	2	Lack of speed	5
System maintenance problems	3	Difficulty accessing	1
Graphics loading time	2	Differing browser capability	2
Training 4			
Lack of training	1	Uneducated users	1
Cumbersome to the untrained	1	Learning to use efficiently	1
E-mail 9			
Email abuse:shotgun messages	2	Sloppy email	1
Unwanted email	5	Unnecessary, spurious communications	1
Access 14			
Lack of Inspector General access	1	Not available to everyone	6
Can't surf Inet fm classified LAN	1	Lack of access control	2
Restricted access to some ".gov" and ".edu" sites	1	Access granted before security policy in place	1
Not enough organized access	2		
Philosophy 18			
Lack of human interaction	4	Misuse by personnel	5
Assumption that everyone wants and needs this technology	2	Over emphasizing mandatory computer use	1
Web potatoes/loss of productivity	5	Privacy concerns	1
***Structure* 10**			
Lack of central reference	1	Non-standard home page layout/usage	1
Too many links	1	Inappropriate" Web pages	1
Changing addresses	1	Hard to find Inet "addresses"	1
Inconsistent scope of material	1	Lack of standardization	1
Sifting the wheat from the majority chaff	2		
***Miscellaneous* 4**			
Non-friendly AFPC want ad format	1	Incomplete information	1
COMSEC/OPSEC violations	1	Potential viruses or tampering	1
No Annoying Aspects 6			

Table D-4. Research Survey Summary, Unsolicited E-mail Types

Email forwards from outside the LAN	1	Religious teachings	2
N/A assignment or promotion info	1	Wants process to restrict "sometimes proper" mail	1
Lost and found notes/lights on	2	Surveys	1
Retirement announcement of stranger	1	Flaming (derogatory, personally-attacking)	1
Inadvertent replies to "ALL"	4	Mail intended for others	1
Any non-discrete shotgun email	6	Chain letters	2
Notice for "Civilians only"	1	Any commercial email	1
Ethnic or sports announcement, special interest	2	Any mail that could have been TELECON	1

Appendix E

User Policy Issues

The following matrix was designed to correlate internet user issues from a representative sample of diverse policies in order to establish common threads of emphasis. Of the seven matrix columns, four represent existing or draft Air Force guidance, two represent existing private sector policies, and one column is devoted to areas specifically addressed in the Research Survey. By inspecting "hits" across the six policy columns, this study drew conclusions about the most popular issues addressed. These popular isues were then compared with subjects that were relevant to the USAF user. They were then divided between user and administrator to form the basis of the subject categories for this report. The Research Study column was added as a reference for survey validation purposes. The internet "User Policy Issues Matrix" (table E-1) ultimately became a key reference in tracing policy origin and formulating policy direction.

Column Key:

A Rinaldi's *Netiquette*
B *Interim Internet Policy* (AF/SCXX)
C Invitrogen *Electronic Mail Etiquette*
D *Tongue & Quill* (draft)
E AFMCI 37-102, *Transmission of Information via the Internet*
F AFMAN 37-126, *Preparing Official Communication*
G Research Survey

Table E-1. User Policy Issues Matrix

	Policies						
Concerns	**A**	**B**	**C**	**D**	**E**	**F**	**G**
Check e-mail daily and limit storage	X	X		X		X	
Delete unwanted messages immediately	X	X		X		X	
Minimize storage in mailbox	X					X	
Extract or download message text to computer for storage	X	X				X	
Never send or store "sensitive" or Classified messages	X	X		X	X	X	
Routinely virus scan your system	X						
Do not maintain "private" messages in common storage	X			X			X
Download telnet instructions for offline viewing	X						
Minimize time on telnet connection	X						
Download screen captured data to local computer	X						
Limit large FTP downloads (1Meg) and attachments for after business hours	X	X		X			
Inquiries to ARCHIE should be in mail form	X						
Pay registration fees for documents or programs	X						
Don't assume posted documents are not copyrighted	X	X					X
Keep messages short and to the point	X	X	X	X	X		
Always include a pertinent "subject" line in e-mail and limit to single subject	X	X		X			
Capitalized letter are considered "shouting"	X		X	X			
Asterisks may be used for emphasis	X		X	X			

Table E-1.—continued

Concerns	Policies						
	A	B	C	D	E	F	G
Avoid control characters	X			X			
Follow chain of command in addressing mail	X	X		X	X	X	
Anticipate possible "forwarding" of your mail	X			X			X
Provide complete citations of copyrighted works	X	X		X			X
Do not forward personal e-mail without permission	X	X		X			X
Be careful with sarcasm and humor—it may not come across	X	X		X			
Use "emoticons"	X		X	X			
Ten Commandments	X						
1. Thou shall not use a computer to harm others	X			X			
2. Thou shall not interfere with other's computer work	X			X	X		X
3. Thou shall not snoop around in other's files	X			X	X	X	X
4. Thou shall not use a computer to steal	X			X			
5. Thou shall not use a computer to bear false witness	X			X			
6. Thou shall not use or copy software for which you have not paid	X			X			
7. Thou shall not use other's resources without authorization	X			X			
8. Thou shall not appropriate other's intellectual output	X			X			X
9. Thou shalt think about the social consequences of the program you write	X			X			
10. Thou shalt use a computer with consideration and respect	X			X			X
Use large mailing lists sparingly		X	X				
Create and use mailing lists to expedite a project		X		X			
Categorize incoming e-mails in folders to aid in future search		X					

Table E-1.—continued

Concerns	Policies						
	A	B	C	D	E	F	G
Never leave an active e-mail terminal unattended		X		X			X
Use a tone of address that is appropriate to recipient		X		X			
Use common abbreviations such as FYI, BTW, etc		X		X			
Send some original text back with reply		X					
Edit thoroughly		X	X	X		X	
Know system restrictions on downloading from various sources		X					
Include a complete "signature" at the bottom of each e-mail	X		X	X		X	
Signature should not be longer than the message			X	X			
Examples of Misinformation			X				
Flaming			X	X			
Defamation			X				
Harassment			X		X		
Obscenity			X				X
Incitement			X				
Circumvention			X				
Impersonation			X		X		
Plagiarism			X				X
Hacking			X				
Viruses and Worms			X				
Security Breach			X		X	X	X
Abuse of property rights			X	X	X		X
Inadequate care of data			X				
Surveillance			X				
Obscuration			X				
"Official Use" restrictions		X		X	X		X
Storing or processing obscene or offensive material					X		X
Permitting an unauthorized person to access a government system					X	X	X

Table E-1.—continued

Concerns	Policies						
	A	B	C	D	E	F	G
Modifying or altering an operating system or configuration without permission					X		
E-mail advantages and disadvantages same: Fast, more people, no paper trail				X			X
Think of message as personal conversation.				X			
Reply to specific addressees only				X			X
Download files only from reputable sites to avoid viruses				X			
E-mails saved and subject to monitoring				X			
Analyze purpose and audience (single subject e-mail)				X		X	
Support your ideas				X		X	
Get organized				X		X	
Use color to show the "bottom line"				X			
Fight for feedback				X		X	
Use large, easy to read fonts				X			
Don't use e-mail for personal ads—put those on a BBS				X			X
Don't send "heavy" files, use >s and ellipses to show reply text				X			
Privacy Act applies						X	X
E-mails must be staffed if applicable						X	
Assign a precedence to e-mails (i.e., routine, immediate. . . .)						X	
Train users on e-mail use						X	

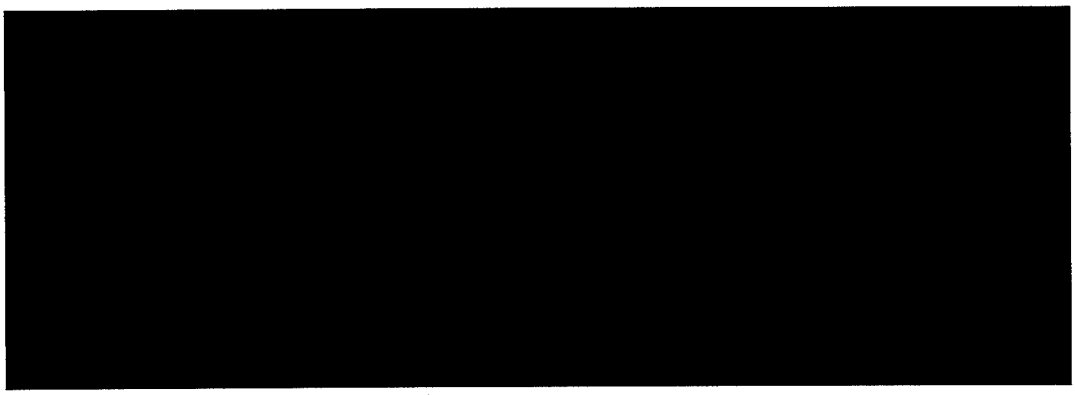
Appendix F

Warning Banner Clarification

Contained within this appendix is correspondence from Headquarters Air Intelligence Agency (AIA/DOX). This correspondence was in response to a series of questions generated by the research team to clear up some apparent inconsistencies that the study uncovered with regard to security warning banners on Web pages.

This study reviewed many Air Force and other DOD Web pages and detected significant inconsistencies, not only in the wording and format of security warning banners, but also in whether the banner was displayed. Some public access Web pages displayed a lengthy, large-font, bold-face warning, effectively intimidating users from accessing the page with its confrontational tone. Public access home pages are meant not only for DOD members, but also for public awareness of interested civilian users.

This study reviewed AFI 33-219, *Telecommunications Monitoring and Assessment Program (TMAP),* in search of the appropriate wording, tone, and intent of the banner. Additional clarification was requested from AIA/DOX. After consultation with the Secretary of the Air Force General Counsel for Military Affairs Office (SSGM), AIA replied with specific answers.



MEMORANDUM FOR AU/RCO
ATTN: Lt Col Kelso

FROM: HQ AIA/DOX
102 Hall Blvd Ste 229
San Antonio TX 78243-7029

SUBJECT: Clarification to AFI 33-219
(Your Memo, 13 December 1995)

1. The information provided herein is in response to your memorandum of 13 December 1995 in which you seek clarification of the banner requirements in AFI 33-219. I regret the delay in getting these answer to you, but your memo broached some areas we felt must be elevated to the Secretary of the Air Force General Counsel for Military Affairs Office (SSGM). Consequently with the holidays at hand and the coordination process involved it simply took longer than normally required to answer the mail. However, I'm confident the end result is a thorough and accurate account which may be used now, as well as for future reference.

2. As a preliminary matter, the focus of AFI 33-219 is on closed Air Force computer systems, not those that are intended for public access. AFI 33-219 was not drafted in contemplation of Internet home pages that are readily accessible to any member of the general public. (For simplicity sake in using this memo as a "ready' reference your question is quoted, followed by SAF/GCM's answer.)

a. Questions 1.a: Is a warning banner required for home pages that are intended for public access and have no options leading to restricted links (e.g., limited to .mil or .af.mil domains)? (The HQ AIA WWW server is an example of this type.)

Answer: No warning banner is required for a home page that is intended to be publicly accessible. However without a warning banner, the legal basis for conducting routine administrative monitoring of computer operations is greatly diminished. There is some limited authority for System administrators to monitor their systems to ensure that they are functioning properly and that only authorized users are accessing them. Clearly

if a publicly available system on the Internet does not require registration or passwords is not encrypted, and does not charge a subscription fee, anyone who can access it is an authorized user. Our only interest in monitoring would be to ensure that such access is not used for an illegal purpose.

b. Question 1.b. For those home pages which do have options leading to restricted links? The warning banner specified in Section C seems a bit harsh for use on a page intended for the general public as well as the military population. Currently the recommended warning banner is: "OFFICIAL U.S. GOVERNMENT SYSTEM FOR AUTHORIZED USE ONLY. DO NOT DISCUSS, ENTER, TRANSFER, PROCESS, OR TRANSMIT CLASSIFIED/ SENSITIVE NATIONAL SECURITY INFORMATION OF GREATER SENSITIVITY THAN THAT FOR WHICH THIS SYSTEM IS AUTHORIZED. USE OF THIS SYSTEM CONSTITUTES CONSENT TO SECURITY TESTING AND MONITORING. UNAUTHORIZED USE COULD RESULT IN CRIMINAL PROSECUTION."

Answer: There is no legal objection to modifying the language of the warning banner for publicly available systems. You are not required to use the precise language in paragraph 16.3.5, AFI-219, on publicly available Air Force home pages.

c. Question 1.c.(1): For home pages that have restricted domains (such as the AETC or DAF home pages) is a warning banner required?

Answer: For home pages that do facilitate access to restricted domains, it is sufficient that the warning banner appear when the user attempts to select the restricted option.

d. Question 1.c.(2): The Department of the Air Force home page (AirForceLINK) is using a variation of the "standard" disclaimer. Is the following a suitable substitute? "This is an unclassified U.S. government computer system, provided as a public service. This system is intended to be used by the government and the public for viewing and retrieving information only. Those parts of the system which do not indicate restrictions are public access. Those parts of the system which have access restrictions are marked with the restriction in parentheses next to the link -you may use any link that is not restricted to you. Your use of this system is subject to monitoring at all times. Unauthorized or illegal activities involving this system can result in criminal prosecution under the Computer Fraud and Abuse Act of 1986."

Answer: You may use a variation of the standard warning banner discussed in paragraph 16.3.5, AFI 33-219. The following language is recommended: *"This is an unclassified U.S. government computer system, provided as a public service. Government personnel and the general public may use this system to review and retrieve publicly available government information. The general public may access any publicly available portions of this system. Selected elements of it are subject to access restrictions that*

are identified in parentheses next to the data link. You may use any portions that do not restrict your access. Anyone using this government system expressly consents to administrative monitoring at all times. You are further advised that system administrators may provide evidence of possible criminal activity identified during such monitoring to appropriate law enforcement officials. If you do not wish to consent to monitoring, exit this system now."

e. Question 1.c.(3): If an option is domain restricted and an authorized user attempts to access it, should the warning banner reappear or is a simple message like "You are not authorized for this option" acceptable?

Answer: It is sufficient if the error message "You are not authorized this option" appears.

f. Question 1.c.(4): If an organization wants to modify the words to the warning banner, who should they consult for approval (AIA/DO, AFC4A, their local JAG)'?

Answer: Recommend that you consult with the servicing Staff Judge Advocates Office to ensure that any proposed warning banner is legally sufficient and provides adequate notice of administrative monitoring.

3. Please do not hesitate to contact us if you require additional information or clarification. My POC for AFI 33-219 and related issues is Ms Andi Calder, DOXI, DSN 969-4491.

cc:
SAF/GCM (Mr Bathen)
HQ AETC/SCTS (Mr Jones)
HQ AIA/JA

Glossary

List of Abbreviations and Acronyms

Term	*Definition*
ACSC	Air Command and Staff College
ADPE	Automated Data Processing Equipment
AETC	Air Education and Training Command
AF	Air Force
AFAF	Air Force Assistance Fund
AFB	Air Force Base
AFC4A	Air Force Command, Control, Communications, and Computers Agency
AFDIR	Air Force Directive
AFH	Air Force Handbook
AFI	Air Force Instruction
AFIN	Air Force Internet
AFIT	Air Force Institute of Technology
AFIWC	Air Force Information Warfare Center
AFMC	Air Force Materiel Command
AFMCI	Air Force Materiel Command Instruction
AFNSO	Air Force Network Strategy Office
AFPAM	Air Force Pamplet
AFPC	Air Force Personnel Center
AFPD	Air Force Policy Directive
AFSSI	Air Force System Security Instruction
AFSSM	Air Force System Security Manual
AIA	Air Intelligence Agency
AIS	Automated Information System
APDP	Acquisition Professional Development Program
ARPA	Advanced Research Projects Agency
ARPANET	Advanced Research Projects Agency Network
ATM	Asynchronous Transfer Mode
BBS	Bulletin Board System
BNCC	Base Network Control Center
C4	Command, Control, Communications, and Computers
CERT	Computer Emergency Response Team
COMPUSEC	Computer Security

Term	*Definition*
COMSEC	Communication Security
DISA	Defense Information Systems Agency
DOD	Department of Defense
DSMC	Defense Systems and Management College
DTIC	Defense Technical Information Center
E-mail	Electronic Mail
FDDI	Fiber Distributed Data Interface
FOIA	Freedom of Information Act
GSA	General Services Administration
HQ	Headquarters
HTML	Hypertext Markup Language
HTTP	Hypertext Transport Protocol
IP	Internet Protocol
ISDN	Integrated Switched Distributed Network
ISP	Internet Service Provider
JAG	Judge Advocate General
JER	Joint Ethics Regulation (DOD 5500.7-R)
LAN	Local Area Network
MAJCOM	Major Command
MILNET	Military Network
NCSA	National Center for Supercomputing Applications
NII	National Information Infrastructure
NIPRNET	Non-secure IP Router Network
NSF	National Science Foundation
NSFNET	National Science Foundation Network
OI	Operating Instruction
OPR	Office of Primary Responsibility
OPSEC	Operational Security
PD	Policy Directive
PDA	Personal Data Assistant
PGP	Pretty Good Privacy
SAF	Secretary of the Air Force
STINFO	Scientific and Technical Information
TCP/IP	Transmission Control Protocol/Internet Protocol
TDY	Temporary duty
URL	Uniform Resource Locator
USN	United States Navy
VRML	Virtual Reality Modeling Language
WAIS	Wide Area Information Server
WWW, Web	World Wide Web

List of Computer Terms

Term	*Definition*
asynchronous	Electronic data that is in a packaged unit and sent out and then received at a later time, much like postal mail.
ATM	Asynchronous Transfer Mode: Format for packaging and transmitting computerized data and images over telephone lines. It can send digitized information at more than 45,000 times the speed available on typical telephone lines. ATM is not an asynchronous transmission technique; transfer mode refers to the switching and multiplexing process. The term asynchronous refers to the fact that cells allocated to the same connections may exhibit an irregular pattern as cells are filled according to demand. ATM supports voice, data, video, and image transmissions; supports multimedia applications; can be used network environments; can handle large data transmissions; and is based on standards.
bandwidth	Throughput or capacity of a network, usually expressed in kilo or megabits per second (kbps, Mbps). The greater the bandwidth, the better the ability to transfer data quickly.
BBS	Bulletin Board System. Utility that allows people to connect to a central computer to upload and download files and to leave messages for other users.
BNCC	Base Network Control Center. Single focal point on each base for providing network management and customer support to critical computer services.
browser	Software program that interprets HTML code, or rather Web pages, and allows users to navigate around the Web.
CERN	European Particle Physics Laboratory (CERN). Research laboratory in Switzerland; originators of the World Wide Web, HTTP, and HTML.

Term	*Definition*
CERT	Computer Emergency Response Team. Formed by Defense Advanced Research Projects Agency (DARPA) in response to needs exhibited during an internet-wide "worm" incident. In November 1988, a worm was released which rapidly brought the internet to its knees when it penetrated over 6,000 internet computers. The CERT Coordination Center (CERT/CC) is located at Carnegie Mellon University's Software Engineering Institute and serves as a focal point for response to internet computer security problems. CERT regularly publishes reports describing computer security incidents.
client	Program that receives information or services from another (the server). Web browsers are clients, because they receive the information they need from the Web servers.
cracker	Person that attempts to break into networks and computers with *malicious* intent and typically causes or attempts to cause damage to information contained on the computer system.
cyberspace	Term used to refer to the entire collection of sites that can be accessed electronically. If a computer is attached to the internet or another large network, it exists in cyberspace. Term often attributed to William Gibson, a young expatriate American living in Canada. He used it as the setting for his early novels and short stories. Additionally, lyricist John Perry Barlow defines it as "that place you are in when you are talking on the telephone."
domain	Highest subdivision of the internet; usually country or by type of organization (such as education, commercial, military, or government).
download	Act of transferring data from a remote computer back to a local computer.
e-mail	Electronic mail. Transmission of information electronically over computer-based systems. E-mail can be used to broadcast a message from a single source to multiple recipients or to collect information from many sources, for example, official records, private communications, and automated transactions.
encryption	Way to secure privacy on networks by the use of complex algorithmic codes.
executable	Critical application file that starts or runs a program.

Term	*Definition*
firewall	Division between a computer network system on the internet and the internet as a whole. Used to limit access to outsiders for security reasons, and to limit the access of the system's users to the outside world.
FTP	File Transfer Protocol. Protocol defining how files are transferred from one computer to another. FTP can be used as a verb to describe the procedure of using FTP. FTP sites, and sites with other protocol standards, can be accessed using Web browsers.
gateway	Portal between two or more networks.
gopher	System, developed by the University of Minnesota, where servers provide a menu system used for accessing specific files. Web browsers can interface with gopher systems.
hacker	Person with a *mischievous* bent who illegally gains access to another's computer system, but does not necessarily cause damage to the computer system.
home page	Top level display of an organization available via the Web. The home page often provides links to other home pages or subordinate or higher level pages within the organization. See also page.
host	Computer connected directly to the internet. An internet service provider's computer is a host, as are computers with permanent connections such as USAF organization's Web servers.
HTML	Hypertext Markup Language. Basic programming code used to create Web pages. These documents are characterized by the .html or .htm file extension, for example, "homepage.html" or "homepage.htm."
HTTP	Hypertext Transfer Protocol. Data transmission protocol used to transfer Web data packages across the internet.
hyperlink	Link in a Web page to information within another Web page. These links are usually represented by hypertext, highlighted or underlined words, or images.
hypertext	See hyperlink.
in-line image	Graphic image that is displayed within a Web or HTML page.

Term	*Definition*
infrastructure	Common-user portion of the base-level command, control, communications, and computer systems environment. It includes transmission, switching, processing, system-control, and network-management systems, equipment, and facilities that support the base. Examples include the base telephone switch and cable plant, base communications center, and local area networks.
internet	Global connection of computer networks and computers. Any computer that can communicate or share information or files with other computers on the common global network is considered "on the internet" or rather, "has access to the internet." The key is that the computer, and therefore a person, *can* communicate in some form with another computer, and therefore another computer, on a *global* basis.
ISP	Internet Service Provider. Company that provides, usually for a fee, a connection to internet.
Java	Web programming language that makes it possible to run small applications remotely over a network, obviating the need for application software residing on the local hard drive. Java applications, or "applets," can be simple spreadsheets or graphic-intensive bouncing balls. Java applets will work equally well regardless of the computer's operating system.
kbps	Kilo (thousand) bits per second.
link	See hyperlink.
local	Physically-close computer or network
Mbps	Mega (million) bits per second.
Mosaic	First popular Web browser, created by NCSA programmers in 1993.
NCSA	National Center for Supercomputing Applications: Located at University of Illinois in Urbana-Champaign, Illinois; released the first popular Web browser, Mosaic, in 1993.
netiquette	Network etiquette conventions used in written communications.
Netscape	Web browser, created by NCSA programmers who subsequently started a company called Netscape Communications.

Term	*Definition*
open specifications	Computer architecture specifications that are not proprietary and are open so that any programmer can write applicable code.
page	Display of an organization available via the Web. A page is subordinate to a home page. The page often provides links to other pages or subordinate pages or higher level pages within the organization.
password	Arbitrary string of characters chosen by a user or system administrator that is used to authenticate the user when attempting to logon to prevent unauthorized access to the account.
privacy	Appropriate conduct of the established network with respect to the user.
protocol	Set of rules that defines how computers transmit information to each other; allows different types of computer and software to communicate.
remote	Physically distant computer or network.
router	Equipment that receives an internet packet and sends it to the next machine in the destination path.
search engine	Program served on some Web servers that searches the internet for specified key words or subjects.
security	Measures to foil unauthorized intrusion on electronic information and hardware by outside elements.
server	Computer that makes information available to other network users. A Web server contains Web pages so that they are available to remote or local users with browsers. The browser asks the server for the page or information, and the server transmits it to the browser.
site	Location where a collection of information is hosted by a server computer on the internet.
surfing	Exploring the internet
synchronous	Electronic data that is exchanged interactively or "real-time."
TCP/IP	Transmission Control Protocol/Internet Protocol. Set of protocols (communications rules) that controls how data is transferred between some computers on the internet.

Term	*Definition*
telnet	Program to allow remote logon to another computer
UNIX	A computer operating system. Many hosts connected to the internet run UNIX.
upload	Act of transferring data from a local computer to a remote computer.
URL	Uniform Resource Locator. Address to a source of information on the internet. The URL contains four distinct parts, the protocol type, the machine name, the directory path and the file name, for example: "http://www.cdsnet.net/vidiot/st-ds9/Preview.html"
virus	Computer program that covertly enters a system by means of a legitimate program, usually doing damage to the system.
WAIS	Wide Area Information Server: Program that searches a group of databases. WAIS can be accessed through the Web.
World Wide Web	WWW, or Web: Distributed hypertext-based information system conceived at CERN to provide its user community an easy way to access global information. The Web is an internet service that enables the internet to browsed using hypertext links. The Web uses HTTP. When a hypertext link is selected, the browser software connects to the specified server (the server could be the local host or could be a remote server) and downloads the information specified by the link at that server site. Once the information is downloaded, the server disconnects until the next hypertext link is selected. The information can be text, graphics, or other multimedia information such as sound or video. Most Web browser software allow the user to access Web sites as well as FTP and gopher sites. The Web is the first technology to allow users with different processors and different operating systems to exchange information freely without the use of expensive "client" software required for client-server applications
worm	Computer program that invades other computers over a network.

Bibliography

AFDIR 33-121, *Compendium of C4 Terminology*, Attachment 1, 5 July 1995.

AFI 33-112, *Automated Data Processing Equipment (ADPE) Management*, 6 May 1994.

AFI 33-114, *Software Management*, 30 June 1994.

AFI 33-115, *Network Management*, 24 June 1994.

AFI 33-219, *Telecommunications Monitoring and Assessment Program (TMAP)*, 12 June 1995.

AFI 35-205, *Air Force Security and Policy Review Program*, 25 February 1994.

AFI 37-131, *Air Force Freedom of Information Act Program*, 16 February 1995.

AFI 37-132, *Air Force Privacy Act Program*, 11 March 1994.

AFI 37-162, *Managing the Process of Printing, Duplicating, and Copying*, 1 December 1994.

AFI 51-303, *Intellectual Property—Patents, Trademarks, and Copyrights*, 25 July 1994.

AFI 61-201, *The Local Scientific and Technical Information Process*, 16 June 1995.

AFI 61-204, *Disseminating Scientific and Technical Information*, 27 July 1994.

AFMAN 37-126, AFMC Supplement 1, 10 July 1995.

AFMAN 37-126, *Preparing Official Communication*, 10 February 1995.

AFMC OI 37-1, *Information Sharing Through the World-wide Web*, 15 March 1996.

AFMC PD 37-1, *Internet Policy*, 19 February 1996.

AFMCI 37-102, *Transmission of Information via the Internet.* [On-line]. Available HTTP: http://www.afmc.wpafb.mil:12000/publications/AFMC_Instructions/37-102.doc [1996, February 21].

AFPAM 36-2705, *Discrimination and Sexual Harassment*, 28 February 1995.

AFPD 31-4, *Information Security*, 1 November 1995.

AFPD 33-1, *Command, Control, Communications, and Computer (C4) Systems*, 17 September 1993.

AFPD 33-2, *Command, Control, Communications, and Computer (C4) Systems Security*, 13 August 1993.

AFSSI 5013, *Password Management,* 15 March 1993.

AFSSI 5021, *Computer Security Reporting Programs Procedures and Formats*, 10 February 1993.

AFSSI 5100, *The Air Force Computer Security (COMPUSEC) Program*, 2 June 1992.

AFSSM 5012, *System Vulnerabilities and Penetration Methods*, 1 October 1991.

AFSSM 5019, *Computer Security User's Guide*, 1 April 1991.

AFSSM 5020, *Remanence Security*, 15 April 1991.

AFSSM 5022, *Network Risk Analysis Guide* (U), 1 March 1993.

Air University Guidelines for Computer and Information Systems (draft), 24 October 1995.

Air University Home Page [On-line]. Available HTTP: http://www.au.af.mil/ [1996, March 25].

America Online's *Rules of the Road* and *Forum Guidelines*, 6 December 1995.

Andrews, Edmund L. (1996, February 9), Communications Law Triggers Lawsuits. *New York TimesFax Internet Edition*, [On-line], p1 (6 paragraphs). Available HTTP: http: http://nytimesfax.com/ [1996, February 9].

Asimov, Isaac. Introduction to *Isaac Asimov's Robot City: Odyssey* by Michael P. Kube-McDowell (New York: Ace Books, 1987).

Assignments Online [On-line]. Available HTTP: http://www.afpc.af.mil/asgnment/htdocs/ [1996, March 18].

AU/RCO. *Synopsis of Written Guidance Concerning the Release of Information via Internet,* no date.

Beach, Darrel, DDN Program Management Office, interview with Maj Matonak, 14 February 1996.

Blackburn, Dave. "Get out your 3D Glasses," *VirtualCity* 1, no. 2 (Winter 1996).

BosniaLINK, Office of Assistant Secretary of Defense Public Affairs. [On-line]. Available HTTP: http://www.dtic.dla.mil/bosnia/ [1996, March 11].

Bucholtz,Chris, "Mind your manners," *Communications International,* May 1995.

Burstein, Daniel. (1992). Photography from Orbit. In *The Risks Digest* (Vol 14, Issue 6, [On-line]. Available HTTP: http://catless.ncl.ac.uk/Risks/14.06.html [1996, April 12].

Carroll, Maj Richard, et al., *Internet: Education and Application for the Knowledge Warrior*, ACSC/DEC/045/95-05, Maxwell AFB, Montgomery, AL: Air Command and Staff College, May 1995.

CERT Coordination Center FTP Server, public directory. Pittsburg, PA: Computer Emergency Response Team/Coordination Center, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA., (no date). [On-line]. Available FTP: ftp://cert.org/pub [1996, March 15].

Chesnut, Jon Ph.D. (jdchesnut@invitrogen.com). (1996, February 14). Invitrogen's E-mail policy. E-mail to Maj Scott Chesnut (71042.664@compuserve.com).

Clearance Procedures for Making Electronic Information Available to the Public, (17 February 1995). DOD Policy Guideline, from the Office of the Deputy Secretary of Defense (Mr John M. Deutch).

CNN Interactive [On-line]. Available HTTP: http://www.cnn.com [1996, February 9].

Cobb, Stephen, "Internet Firewalls," *Byte*, October 1995.

Coffman, Commander Homer, ACSC/DT, Maxwell AFB AL, interview with Maj Jon Link, 7 February 1996.

CompuServe Information Service *Operating Rules*. CompuServe, Columbus, Ohio. [On-line] Available CompuServe: GO Rules [1996, February 27].

Connelly, Jim, "Royal Stings," *websight,* issue 1.

Consumer Survey of WWW Users, Preliminary Results from 4th Survey (12 December 1995). [On-line]. Available HTTP: http://www.www.cc.gatech.edu/gvu/user_surveys/survey-04-1995 [1995, December 20].

Cooper, Pat "Computer Hackers Beware," *Air Force Times*, 2 October 1995.

Dery, Mark, "uplist," *VirtualCity* 1, no. 2 (Winter 1996).

Determining the Status of Cyberjournalists in Washington. *New York TimesFax* (Internet edition). [On-line] Available HTTP: http://nytimesfax.com [1996, February 26].

Deutch, John M. (17 February 1995) *Clearance Procedures for Making Electronic Information Available to the Public.* DOD Policy Guideline, from the Office of Deputy Secretary of Defense [On-line]. Available HTTP: http://www.dtic.dla.mil/defenselink/memo.html [1996, March 26].

Deutch, John M. (5 May 1995) *Open Computing Architectures.* DOD Policy Guideline, from the Office of Deputy Secretary of Defense [On-line]. Available HTTP; http://www.afmc.wpafb.af.mil:12000/organizations/HQ-AFMC/SC/scp/internet-policy/secdef.htm [1996, March 26].

Discussion on *Star Trek: Generations.* [On-line] Available UseNet: alt.startrek.creative [August 1994].

DOD 5200.1, *DOD Information Security Program*, 7 June 1982.

DOD 5200.21, *Dissemination of DOD Technical Information*, 27 June 1982.

DOD 5200.28-STD, *Department of Defense Trusted Computer Evaluation Criteria* ("Orange Book"), 26 December 1985.

DOD 5230.9, *Clearance of DOD Information for Public Release*, 2 April 1982.

DOD 5500.28, *Security Requirements for Automated Information Systems (AIS)*, 21 March 1988.

DOD 5500.28-STD, *Department of Defense Trusted Computer Security Evaluation Criteria*, 26 December 1985.

DOD 5500.7-R, *Joint Ethics Regulation*, August 1993. (paragraph 2-301—Use of Federal Government Telephone systems)

Draft Inputs for *Tongue and Quill*, Use of the internet and e-mail.

Elmer-Dewitt, Philip. "Why Java is Hot," *Time*, 22 January 1996.

Fed Center (1995). The Interfed Group. [On-line]. Available HTTP: http://www.fedcenter.com [1996, March 26].

French Book Banned, Then Pirated. *New York Times,* 18 March 1996, A1. [On-line]. Available via Edupage List: listproc@elanor.oit.unc.edu [1996, March 20].

Groupware or Webware? *Wall Street Journal,* 7 November 1995, A1. [On-line]. Available via Edupage List: listproc@elanor.oit.unc.edu [1995, November].

Gunther, Marc, "Goofing off at the office goes high-tech." *Montgomery Advertiser*, 24 March 1996.

Hall, Mr. Charles, Systems Engineer, Silicon Graphics Corporation. Briefing to ACSC students, 13 December 1995.

Hauptman, Robert and Susan Motin, "The Internet, cyberethics, and virtual morality," *Online,* March 1994.

Hertzbert, Robert, "Java Picks Up Steam," *WebWeek* 2, no. 1, January 1996.

Higher Ed Groups Eye Electronic Copyright Bill. *Chronicle of Higher Education*, 16 February 1996, A26. [Online] Available via Edupage List: listproc@elanor.oit.unc.edu [1996, February 18].

HKK. (1995, February 14) Dennis Erlich Rumors. *Discussion on the Erlich Case.* [On-line]. Available HTTP: http://www.eff.org/pub/Legal/Cases/CoS_v_the_Net/cos_raids_erlich_ 021495.statement [20 March 1996].

Howells, Mike. (no date). "*EJECT! EJECT! EJECT!*" *(full transcript of e-mail written by Scott Zobrist, wingman of pilot who first made contact with downed F-16 pilot Scott O'Grady in Bosnia, original e-mail date 8 Jun 1995)*, [On-line]. Available HTTP: http://www.i1.net/~mhowells/eject.html [1996, March 10].

Intelink Concept of Operations for AF-wide Implementation (draft), AIA/SCXP, 25 July 1995.

International Copyright Conference. *Financial Times,* 14 February 1996, p7. [Online]. Available via Edupage List: listproc@elanor.oit.unc.edu [1996, February 18].

IRS Home Page. [On-line]. Available HTTP: http://www.irs.ustreas.gov [1996, January 15].

Jacobsen, Kristin, "Time To Put the Internet in Perspective," *C&RL News*, March 1995.

Java: Programming for the Internet, 1995, Sun Microsystems, Inc Mountain View, CA, [On-line]. Available HTTP: http://JAVA.SUN.COM [1996, March 26].

Kaliwai, Lt Col George III (USAF), "Surfing the Third Wave," prepared for completion of National Defense Fellowship Ohio State University, July 1994.

Kanagaki, Ken, MITRE (AIA/SCM), Kelly AFB TX, interview with Maj Matonak February 1995.

Kelso, Mrs Nancy. AU Home Page Curator, Maxwell AFB AL, interview with Maj Smith 8 December 1995.

Kim, James. "Security flaw found in new Netscape software," *USA Today,* 22 February 1996.

Krimmel, Kris. (kkrimmel@sagate1.kelly.af.mil). (1996, February 28). Applet Enabled Browser Moratorium Issued at Kelly. E-mail to Multiple recipients of list <www@infosphere.safb.af.mil>.

Laquey, Tracy. *The Internet Companion.* 2nd ed. New York: Addison-Wesley Publishing Company, 1994.

Lewis, Peter H., "AT&T Unveils Ambitions Internet Plan," *New York TimesFax Internet Edition*, 28 February 1996.

Library of Congress Home Page (2 February 1996) [On-line]. Available HTTP: http://www.loc.gov [1996, February 17].

Livingston, Col, AIA/DOX, to Lt Col Kelso, AU/RCO, letter, subject: Clarification to AFI 33-219 (Your Memo, 13 December 1995), 2 February 1996.

McDowell, Maj Phil (mcdowep@WPGATE1.wpafb.af.mil). (1996, February 21). re: Policy and Security Issues. E-mail to Maj Jon Link (jlink@MAX1.au.af.mil).

McDowell, Maj Phil (mcdowep@WPGATE1.wpafb.af.mil). (1996, February 28). re: more internet questions. E-mail to Maj Jon Link (jlink@MAX1.au.af.mil).

Miller, Col. AF/SCXX (millerb@afsync.hq.af.mil). (1996, February 28) Interim Internet Guidance (draft). E-mail to Maj Matonak (amatonak@max1.au.af.mil).

Mixon, Bobbie ASC Public Affairs, "Agents seize computers, suspect hacking," *Skywrighter*, 4 March 1994.

Montgomery, Capt Kenneth, ACSC/DTT, interview with Maj Smith, 21 December 1995.

National Science Foundation, *Acceptable Use Policy,* 17 January 1995.

NIST Special Pub 800-10, National Institute of Standards and Technology [On-line]. Available HTTP: http://csrc.ncsl.nist.gov/nistpubs/800-10/ [1996, January 17].

Parental Control Software Effectively Monitors Employee's Internet Activity—Improves Productivity (26 March 1996). *PR Newswire*. [On-line via PointCast Network]. Available HTTP: http://pcn.com [1996, March 26].

Parental Controls. CompuServe, Columbus, Ohio.[On-line] Available CompuServe: GO Controls [1996, February 13].

Perini, Col Michael, HQ ACC/PA, briefing to ACSC students and faculty on 11 March 1996.

Personal Home Page Publishing Service. CompuServe, Columbus, Ohio. [On-line] Available HTTP: http://ourworld.compuserve.com [1996, February 12].

Pethia, Richard D. and Kenneth R. van Wyk, *Computer Emergency Response—An International Problem* (1990, November 14) Pittsburg, PA: Computer Emergency Response Team/Coordination Center, Software Engineering Institute Carnegie Mellon University, Pittsburgh, PA. [On-line]. Available HTTP: http://www.riken.jo.jp/archives/security/cert/info/security.response.cert.txt [1996, February 28].

Position Paper on the Information Project Barrier Reef, AFC4A, 5 January 1996.

Privacy, Invasion of. (1993) *New Grolier Multimedia Encyclopedia*, (Release 6), [CD-ROM].

Quarterman, John "Internet Growth," *Matrix News* 3(12), December 1993.

Quarterman, John, "What is the Internet, Anyway?" *Matrix News*, 4(8), August 1994.

Ramos, Joshua Cooper, "How Cheap Can Computers Get?" *Time*, 22 January 1996.

RealAudio, Audio-on-demand for the Internet, (22 Mar 1996), Progressive Networks, Seattle WA. [On-line]. Available HTTP: http://www.realaudio.com [1996, March 26]

Results from the First World Wide Web User Survey (Jan 1994) [On-line]. Available HTTP: http://www.www.cc.gatech.edu/pitkow/survey/survey-1-1994/survey-paper.html [1996, March 7].

Rinaldi, Arlene H. (1995) *Computer Network Policy* [On-line]. Available HTTP: http://www.fau.edu/rinaldi/net/netpol.txt [1996, February 9].

Rinaldi, Arlene H. (1995). *The Net: User Guidelines and Netiquette* [On-line]. Available HTTP: http://www.fau.edu/rinaldi/netiquette.html [1996, March 26].

SAF Memo, *Clearance Procedures for Making Electronic Information Available to the Public*, 25 May 1995. Memorandum for ALMAJCOM-FOA/CC, from the Office of the Secretary of the Air Force (Ms Sheila E. Widnall).

SAF/AQT Memo, *Use of Internet for Transmitting or Providing Access to Unclassified, Limited Distribution Information*, 12 December 1994.

Scherr, Edmund F. (1995, September 5) *U.S. Outlines Safeguards for Intellectual Property Rights*, [On-line]. Available HTTP: http://sunsite.nus.sg/usis/New/Update/090595.html [1996, February 9].

Schiller, Jeffrey I. *MIT Distribution Site for PGP*. (1995). [On-line]. Available HTTP: http://web.mit.edu/network/pgp.html [1996, March 26].

Schu, Capt (USN), briefing to ACSC students/faculty, "Information Warfare" 29 November 1995

Shimomura, Tsutomu and John Markoff, Catching Kevin, *Wired*, February 1996.

Stank, David J. and Sylvia Moon, *Network Security Secrets*, IDG Books Worldwide Inc, San Mateo CA, 1993.

Stehle, Tim. *Getting Real About Usage Statistics*, [On-line]. Available HTTP: http://www.infi.net/ naa/stehle.html [1995, December 15].

Sterling, Bruce; *The Hacker Crackdown,* [On-line]. Available HTTP: http://www.eecs.nwu.edu/ hacker_crackdown/ [1996, January 15].

Stoll, Clifford, *The Cuckoo's Egg*, New York, NY: Doubleday, 1989

Templeton, Brad. (1994). *10 Big Myths about Copyright Explained,* [On-line]. Available HTTP: http://www.clari.net/brad/copymyths.html [1996, February 21].

The Report of the Working Group on Intellectual Property Rights (1995). [Online]. Available HTTP: http://www.uspto.gov/web/ipnii/ [1996, March 20]

The World Wide Web Consortium, [On-line]. Available HTTP: http://www.w3.org/ pub/WWW/.

This Is The Web—It's Not A Reading Room (*Washington Post,* 12 November 1995, C5) [On-line]. Available via Edupage List: listproc@elanor.oit.unc.edu [1995].

Toffler, Alvin and Heidi, *War and Anti-War* (New York: Warner Books, 1995).

Tolhurst, William A et al. *Using the Internet* Special ed. Indianapolis: Que Corporation, 1994.

Top 5% of the Web (1996) Lycos Inc. [On-line]. Available HTTP: http://www.pointcom.com/ [1996, March 26].

University of Michigan Business School. (12 December 1995). *Consumer Survey of WWW Users, Preliminary Results from 4th Survey,* [On-line]. Available HTTP: http://www.www.cc.gatech.edu/gvu/user_surveys/survey-04-1995 [1995, December 20].

Webossary [On-line] Available CompuServe: go www [1995, December 23]

What's New? CompuServe, Columbus, Ohio. [On-line] Available CompuServe: GO Telecom [1996, February 27].

White House Home Page, [On-line]. Available HTTP: http://www1.whitehouse.gov/ WH/ welcome.html [1996, February 17].

White, Col Charles, memorandum for record, subject: AU Copyright Conference, 27 July 1995.

Wietse Venema and Dan Farmer (24 April 1995). *Security Administrator's Tool for Analyzing Networks* [On-line]. Available HTTP: http//www.fish.com/satan/ [1996, March 16].

YAHOO. [On-line]. Available HTTP: http://www.yahoo.com [1996, February 9].

Zakon, Robert Hobbes. *Hobbes' Internet Timeline, v2.2* [On-line]. Available HTTP: http://info.isoc.org/guest/zakon/Internet/History/HIT.html [1995, December 14].

Index